Strategic Change

WILEY

RESEARCH ARTICLE OPEN ACCESS

Strategies and Process of Trade Secret Misappropriation Mitigation: The Case of UK

Oleksandra Ozcan[1,2] | David Pickernell[1]

[1]School of Management, Swansea University, Swansea, UK | [2]School of Languages and Applied Linguistics, University of Portsmouth, Portsmouth, UK

Correspondence: Oleksandra Ozcan (oleksandra.ozcan@port.ac.uk)

Received: 10 July 2024 | **Revised:** 3 April 2025 | **Accepted:** 16 April 2025

Keywords: dynamic capabilities | trade secret misappropriation | trade secret misappropriation-mitigation process | trade secret mitigation strategies

ABSTRACT

Trade Secrets (TS) are vital for innovation-driven companies, and their loss can inflict significant financial and reputational damage, particularly in the absence of established policies to mitigate misappropriation in the UK. The current academic literature lacks detailed strategies for firms to effectively address these threats. This paper aims to bridge the research gap by conducting interviews with industry professionals and analyzing UK legal cases related to TS misappropriation. By integrating findings within the Dynamic Capabilities (DC) theoretical framework, we develop a more comprehensive approach to mitigating TS misappropriation, thereby enhancing the detail and relevance of DC approaches in the TS context. This research, therefore, not only offers practical strategies for companies in the UK to prevent future breaches but also advances academic understanding of the process of TS misappropriation-mitigation and outlines potential directions for further inquiry in this area.

1 | Introduction

Trade secrecy is one of the most widely used intellectual property (IP) protection mechanisms in the UK, utilised by organisations of all sizes. It is a highly valuable asset to any business (Andersen and Striukova 2010; Searle 2021). In comparison to patents and other forms of IP protection, Trade Secrets (TS) possess a weaker protection regime, making owners more vulnerable to theft and misappropriation (Ozcan et al. 2023), the global costs associated with TS loss amounting to almost 3% of developed economies' GDP (Passman 2014). For many businesses, loss of a TS also constitutes loss of competitive advantage, the potential loss or exposure of specific confidential technological inventions creating uncertainty in business and a slowdown in innovation (Santiago 2017; Khan et al. 2021; Shiau et al. 2023).

Businesses are often, however, unaware of the strategies to follow in the event of TS misappropriation or theft, the recent number of high-profile cases of TS misappropriation in the UK highlighting: (1) poor TS management practices; and (2) lack of understanding of the misappropriation–mitigation process (Ozcan et al. 2023). Although the UK government has clarified the definition of a trade secret (TS) in the Trade Secrets Regulation (2018) and liability for TS theft in the National Security Act (2023), no clear policy or set of recommended actions exists for businesses on how to respond to TS misappropriation. Misappropriation–mitigation strategies and processes therefore need further development, the World Intellectual Property Organization (WIPO) itself calling for stronger policy frameworks for TS management and effective mechanisms for addressing TS misappropriation (WIPO 2022).

Whilst TS have long been part of the academic discourse (see, for example, Gerle and Varsányi 1997), in the scholarly literature, TS misappropriation is usually mentioned as an outcome of failed efforts at TS protection (Hannah 2005; Basuchoudhary and Searle 2019; Ozcan et al. 2023). Bos et al. (2015) view TS misappropriation-mitigation as a final stage of the TS lifecycle. Ozcan et al. (2023) see misappropriation-mitigation as part of TS management, identifying mitigation approaches applicable to organisations in times of TS misappropriation, whilst Diestre et al. (2023), discuss the implications of IP infringement after its

Key Points

- There is an urgent and significant gap in existing trade secret management practices and academia regarding the mitigation of trade secret misappropriation.
- The research proposes a practical and step-by-step process for mitigating trade secret misappropriation, based on Dynamic Capabilities (DC) theory, offering specific actions for sensing, seizing, and reconfiguring in response to misappropriation threats.
- The proposed process offers practical guidance to managers on how to enhance organizational resilience and maintain competitive advantage. This guidance is a direct result of the research's focus on the practical implications of mitigating trade secret misappropriation.

occurrence and litigation, arguing for development of anti-trust policies to mitigate collusion and prevent further instances of IP infringement. Conversely, Hannah (2005) argues that lack of trust between employees and employers drives TS misappropriation. Hannah (2006) identify the lack of understanding of what constitutes TS protection and the signing of NDAs by employees as potential causes of misappropriation.

Finally, the study of Maurer and Zugelder (2000) argues for the development of specific HR strategies to safeguard TSs and confirm the importance of security culture and employee loyalty in preventing TS misappropriation, Hannah (2005, 2006) identifying trust building, training, and frequent communication about TS policies between the organization and the employees as decreasing the chances of the loss of TS. Finally, Basuchoudhary and Searle (2019) focus on the issues of TS theft and the development of efficient compliance systems within organisations. The authors in these studies, however, all argue for further exploration of the final stages of TS management, specifically the mitigation of TS misappropriation.

Given that this is the state-of-the-art in the existing literature (explored in greater detail in Section 3), a study considering TS misappropriation-mitigation as a step-by-step process within the TS management framework is consequently needed to close this research gap. The goals of the study are therefore: to identify the strategies and methods used during the mitigation of TS misappropriation, including that resulting from cyber theft, and which are most effective; To map the TS management processes that exist, particularly mitigation management processes, as the final stage of a TS lifecycle; To evaluate which specific policies, procedures, and strategies, including informal strategies, are most likely to be effective in responding to TS misappropriation and the loss of valuable information, and the potential improvements that can be made to prevent future instances; to review how critical organizational reactions to the breakage of the secrecy regime and subsequent organizational strategies are in preventing initial and further misappropriation of intellectual property (IP) assets, thereby offering a hopeful outlook for the future.

To achieve this, a sequential qualitative mixed-methods approach is employed (Morse 2010), utilizing data derived from 18 carefully selected legal cases involving TS misappropriation in the UK and 12 interviews with industry professionals. The data was analysed according to the research questions and the theoretical lens using thematic analysis and NVivo software (Braun and Clarke 2014), with Dynamic Capabilities (DC) providing the theoretical framework for the process of TS misappropriation–mitigation (Teece 2007).

The findings in this study indicate a low level of understanding of the actions needing to be undertaken by organisations after a TS misappropriation threat or misappropriation. Adapting DC theory, we establish a step-by-step process of TS misappropriation-mitigation: Step 1—implementation of TS protection; Step 2—sensing TS misappropriation; Step 3—seizing TS misappropriation; and Step 4—TS reconfiguration. Hence, our paper offers both theoretical and practical contributions. We contribute to the overall literature on intellectual property protection by providing a DC-based theoretical framework for TS misappropriation-mitigation (Hemphill 2004; Fang et al. 2017; Crittenden et al. 2015; Fedorenko et al. 2023). We extend future research directions of Bos et al. (2015), Ozcan et al. (2023), Wang (2021), Wang et al. (2023), and Diestre et al. (2023) and investigate in detail the stages of TS misappropriation-mitigation and prevention strategies. Based on our practical contributions, we provide organisations with coherent, step-by-step guidance on how to respond to TS misappropriation or misappropriation. This process enables organisations to navigate TS misappropriation with flexibility and confidence, ultimately increasing the protection of TSs and valuable confidential information in the future.

The paper is structured into a theoretical background, literature review, research questions, methodology, and then results. The paper concludes with discussions, conclusions, theoretical and practical contributions, limitations, and further areas of research.

2 | Theoretical Background

TS can generate a competitive advantage (Crittenden et al. 2015), with trade secrets potentially determining organizational success or failure (Hemphill 2004). Considering the study by Ozcan et al. (2023) in the context of TS misappropriation-mitigation, DC theory provides a potentially relevant theoretical background, particularly given its longstanding association with strategy (McGuinness and Morgan 2000). The constructs and variables subsequently identified and used are grounded in DC theory and the literature. As Ozcan et al. (2023) also identify, however, in the case of TS, there is a need to integrate the Resource-Based View (RBV) into the initial stage of TS identification and protection, as demonstrated in Figure 1 below.

Using RBV first, Ozcan et al.'s (2023) systematic literature review identifies that a TS must be valuable, rare, inimitable, and organized within the company. It must thus be well protected as a key organizational resource capable of generating a competitive advantage. According to DC theory, to maintain a competitive advantage in the market, organisations need to be adaptable to external environmental changes, which is essential for sustained profitability. Sustaining competitive advantage progresses through sensing, seizing, and reconfiguring (Teece 2007). In traditional DC theory (Teece 2010), sensing

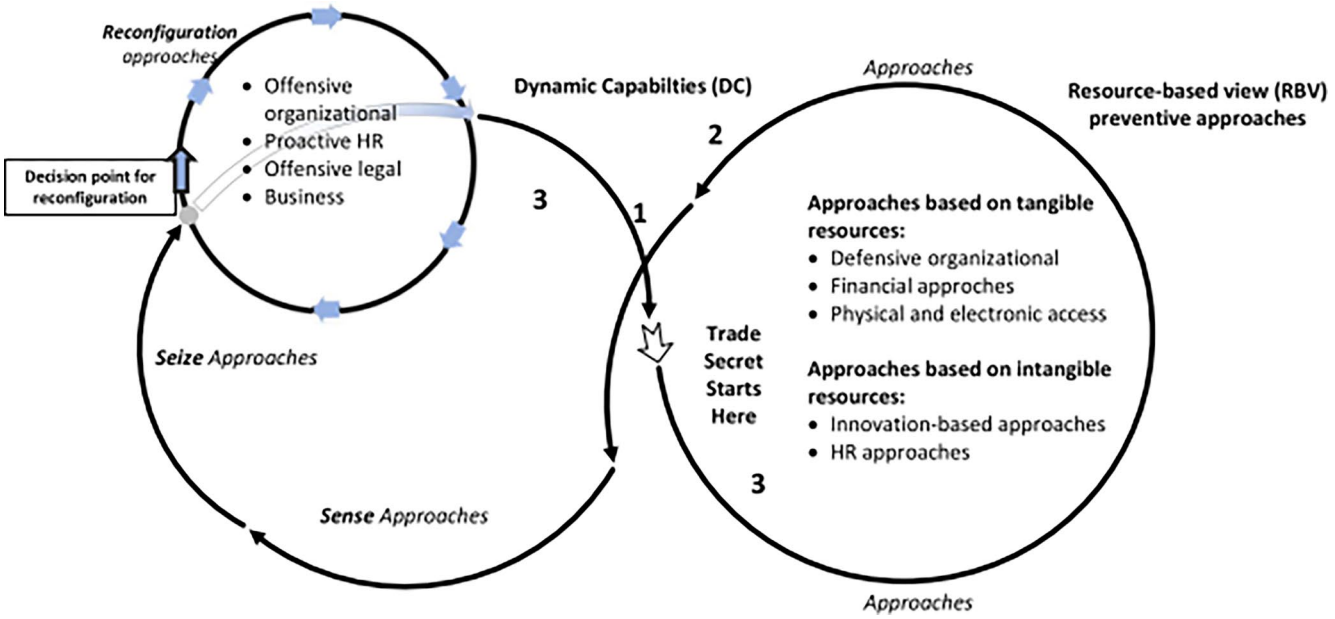

FIGURE 1 | Theoretical underpinning of TS approaches (Ozcan et al. 2023). [Color figure can be viewed at wileyonlinelibrary.com]

involves learning, filtering, shaping, and calibrating potential opportunities and threats. Seizing pertains to capitalizing on identified opportunities by developing new products, processes, or services, often leading to enhanced research and development efforts. Reconfiguring is then about the capability to rearrange and adapt assets and organizational structures to align the company's internal operations with the opportunities that have been seized.

In the case of TS mitigation, sensing refers to the organization's ability to anticipate potential threats to TSs and other forms of intellectual assets. The seizing stage entails organizational adaptations to possible threats or loss of a TS. Finally, the reconfiguration stage involves readjusting the company to the new environmental circumstances (loss of a Total Strategy, TS) to maintain a competitive advantage or create a new TS or other form of Intellectual Property (IP) for competitive advantage (Teece 2007; Barreto 2010).

With the DC theory in mind, Al-Aali and Teece (2013) propose a more integrated approach to IP management. The authors argue that, for the IP management process to be efficient, it must be integrated into the company's overall corporate strategy and business model. If IP assets are a prerequisite for a company's competitive advantage, it is therefore critical that TS are identified through an IP audit process. The TS misappropriation-mitigation process therefore requires, as a first step, the establishment of a protection approach, followed by predefined organizational steps (see Figure 2).

Figure 2 above illustrates that TS misappropriation-mitigation begins with TS protection, as part of the TS management process. The existence of a protection framework provides a foundation and starting point for the sensing, seizing, and reconfiguring stages. If such a TS protection framework is not in place, the mitigation process is not likely to succeed, and the TS will be lost. It is worth noting, however, that TS misappropriation-mitigation does not guarantee that the TS will not be lost. Instead, it provides an action plan if the threat arises.

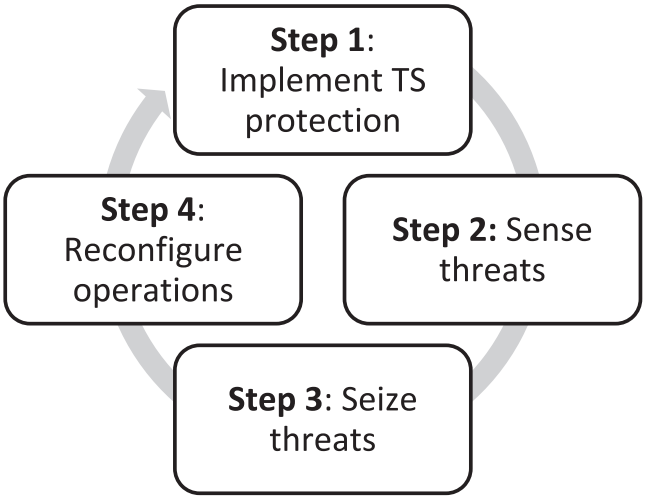

FIGURE 2 | A conceptual framework for the DC theory-based TS misappropriation-mitigation process.

The TS misappropriation-mitigation framework, as presented in Figure 2, is a multifaceted process. It requires alignment with all organizational functions to mitigate the threat or loss of a TS, encompassing the DC theory stages that need to be maintained by employees and integrated into the overall TS management process and the organization's business strategy. DC theory itself, however, is not without criticisms (Collis et al. 2021), not least because of the need to contextualize the DC framework within the specific context it is being used in (Gremme and Wohlgemuth 2017), concerning the impacts of contingency conditions (Barreto 2010), and the potential for there to be different types of DCs within different strategic settings (Vu 2020). Consequently, while believing DC to be an appropriate general framework for analysing TS

TABLE 1 | Key literature on TS management.

Key literature	Areas of research	Identified literature gap
Epstein and Levi (1987)	Examination of the TS protection strategies	There is a gap in understanding effective strategies for mitigating TS misappropriation
Bos et al. (2015)	TS lifecycle. Advantages and disadvantages of a TS	There is a gap in research regarding the full spectrum of TS management processes. The study recommends an in-depth examination of mitigation as the final stage of the TS lifecycle
Basuchoudhary and Searle (2019)	Organizational strategies against cybercrime and economic espionage	The study recommends further research into the policies and strategies for addressing TS misappropriation resulting from cyber theft across various countries and jurisdictions
Wang (2021)	IP strategies and employee relationships	The study suggests further empirical research to explore the effectiveness of informal IP strategies and how they can be improved to prevent instances of TS and valuable information loss
Ozcan et al. (2023)	The study explores strategic approaches to TS management	The study recommends further investigation into strategies and processes for mitigating TS misappropriation
Wang et al. (2023)	The study explores offensive patent litigation	There is a gap in understanding the importance of organizational strategies in preventing the misappropriation of intellectual property (IP) assets
Fedorenko et al. (2023)	The study explores and summarizes studies in the area of trade secrecy and its use	The study emphasizes the importance of organizational reaction to the breakdown of the secrecy regime. The authors argue for the establishment of specific policies and procedures in such circumstances

misappropriation-mitigation, the study will also enhance the understanding of specific DC processes in this context. With this clear DC-framed theoretical basis, the study is therefore connected to the broader academic discourse, maximizing its potential contribution to the field.

3 | Literature Review

As stated in the introduction, the literature on TS misappropriation-mitigation is not well established; Table 1 presents an analysis of the current state-of-the-art in debates.

According to the more recent literature, as shown in Table 1, Bos et al. (2015) establish a TS management lifecycle. If unwanted exposure of the TS occurs, it is in the interest of the organization to mitigate the adverse effects of such exposure. This mitigation effort encompasses affirmative action, including formal and informal responses. Formal mitigation measures can include litigation or internal TS protection approaches if there is evidence of a violation of internal procedures. Informal measures are less well represented, but one example is the strategic dissemination of false information to distract attention from misappropriation and deceive external partners. Bos et al. (2015) also argue, however, that further exploration of the later stages of TS protection management, both before and after misappropriation, is needed, with more research required to identify the taxonomy of mitigation approaches and their effectiveness.

Wang et al. (2023) focus on offensive IP (intellectual property) protection strategies before litigation. According to the authors, early identification of IP infringement requires maintaining organizational protection processes and an efficient intellectual property rights compliance system. This ensures lower management costs and cognitive efforts in the event of violation of intellectual property rights. This follows on from Epstein and Levi's (1987) study, in which the authors discuss the inefficiencies of defensive TS protection strategies, highlighting the necessity for proactive, continuous TS audits. According to Epstein and Levi (1987), TS audit can be an effective measure in TS misappropriation-mitigation that proves "reasonable measures of protection" during litigation and

prevents TS leaks, Basuchoudhary and Searle (2019) illustrating both the importance of cyber security in theft mitigation and prevention and TS cyber theft underreporting due to the fear of further exposure.

Much TS protection and misappropriation research is also focused on HR (human resources). The lack of employee commitment and high employee mobility are one of the main reasons for TS misappropriation (Wang 2021). Wang (2021) argues that informal IP strategies are seldom efficient. The root cause of TS misappropriation often stems from the mobility of employees and the temptation to exploit confidential knowledge for personal or competitive gain. Merely relying on non-disclosure agreements (NDAs), which employees may disregard or circumvent, leaves companies vulnerable. Combining NDAs with non-compete clauses or TS laws, however, creates a stronger deterrent, as violations can result in legal consequences. Ultimately, companies must complement their legal safeguards with proactive measures to foster a culture of loyalty and security consciousness among employees.

It is evident, however, that more research is needed, specifically in exploring effective organizational mitigation processes after the occurrence of misappropriation. This research aims to fill the existing literature gap by providing a method for mitigating TS and the approaches organisations undertake to maintain their TS or mitigate the negative consequences of TS loss.

4 | Research Questions

In light of the theoretical foundations presented in Section 2 and the literature gaps identified in Section 3, this paper aims to provide a more detailed description of the stages involved in mitigating TS misappropriation within the overall process of TS management. Synthesizing the gaps in the literature presented in Table 2, the goals of the study are therefore: to identify the strategies and methods used during the mitigation of TS misappropriation, including that resulting from cyber theft, and which are most effective; To map the TS management processes that exist, particularly mitigation management processes, as the final stage of a TS lifecycle; To evaluate which specific policies, procedures, and strategies, including informal strategies, are most likely to be effective in responding to TS misappropriation and the loss of valuable information, and the potential improvements that can be made to prevent future instances; to review how critical organizational reactions to the breakage of the secrecy regime and subsequent organizational strategies are in preventing initial and further misappropriation of intellectual property (IP) assets.

The novelty of the paper's goals is, therefore, to bridge the gap in the current academic literature regarding established misappropriation-mitigation policies in the UK. The consequent relevance of the paper's goals is in identifying strategies for firms to address TS misappropriation threats more effectively. The DC-based processes sought to serve as practical guidance for managers to better enhance organizational resilience and sustain competitive advantage through step-by-step guidance for organizations to follow in the event of TS misappropriation. We therefore intend to answer the following questions:

TABLE 2 | Thematic analysis process of the legal cases (Adopted from Rojon et al. 2021).

Step	Action
1.	Preliminary case search
2.	Identification and screening of data from BAILII ($n = 5528$) based on the key term "TS"
3.	Reading of factual background and application of ***exclusion and inclusion*** criteria: TS misappropriation or a breach of confidential information; UK jurisdiction; cases not older than 25 years ($n = 108$)
4.	Reading of full case ($n = 108$). Exclusion of full text cases based on the breach of confidential information/TS ($n = 52$). Further exclusion of full text cases based on the identification of TS protection approaches after misappropriation ($n = 18$).
5.	Familiarization with the selected legal case data in NVIVO (Tranfield et al. 2003). Identification of initial themes in the cases (facts, parties to dispute, breach circumstances, etc.).
6	Structural coding and generation of initial codes from legal cases (*TS management process, stages of TS management, TS management approaches*).
7.	Search and review of legal case themes in Nvivo
8.	Use of intercoder reliability to define legal case themes in Nvivo (*TS misappropriation-mitigation stages; TS misappropriation-mitigation measures*).
9.	Consolidation and refining of the results.
10.	Writing up and presentation of findings

Note: Following the screening 18 cases, were selected for an entire case reading and analysis (Pittaway et al. 2004), using the stages outlined in steps 5–10.

1. What strategies and processes are used during the mitigation of TS misappropriation, including that resulting from cyber theft, and which are most effective?
2. What TS management processes exist, particularly mitigation management processes, as the final stage of a TS lifecycle?
3. Which specific policies, procedures, and strategies, including informal strategies, are most likely to be effective in responding to TS misappropriation and the loss of valuable information, and what potential improvements can be made to prevent future instances?
4. How important are the organizational reactions to the breakage of the secrecy regime and subsequent organizational strategies in preventing initial and further misappropriation of intellectual property (IP) assets?

5 | Methodology

This study employs a (two-step) sequential qualitative mixed method approach (Morse 2010). The first step involves a thematic

TABLE 3 | List of interviewees.

Interviewee	Age	Highest level of education	Position in organization	Years of experience
X1	60	BA	Head of IP	15+
X2	45	BA	Head of IP	20+
X3	50	BA	Head of IP	5+
X4	35	BA	Director	5+
X5	60	BA	Head of IP	20+
X6	35	MA	Director	10+
X7	50	PhD	Head of IP	20+
X8	50	PhD	Head of IP	15+
X9	60	PhD	Director	15+
X10	50	BA	Head of IP	20+
X11	50	PhD	Head of IP	20+
X12	45	MA	Head of IP	10+

analysis of UK legal cases on TS misappropriation (Tranfield et al. 2003). The second step provides a thematic analysis of semi-structured interviews with industry experts (Jogulu and Pansiri 2011).

The themes in the data were identified in NVIVO following Braun and Clarke's thematic analysis process (2006). The identification and tailoring of NVIVO analysis results to the parameters of DC theory was identified with the acknowledgement of uncertainties in the environment of the innovating companies implementing trade secrecy. Verification of themes was achieved by means of cross data-verification between the interviews and legal cases and refinement through iteration (Ozcan et al. 2023).

5.1 | Legal Cases Analysis

To capture relevant cases, the study adapted Tranfield et al.'s (2003) case analysis guidelines, searching for cases using the BAILII (British and Irish Legal Information Institute) database, and filtered by initial relevance using the keyword "TS". The inclusion criteria, adapted from Rojon et al. 2021, and outlined in the first four steps in Table 2, were then applied to obtain a controllable data set. The fourth step of the screening process, crucially, included reading the factual backgrounds with the application to ensure the cases selected were those clearly demonstrating breach of a TS and included information concerning TS protection approaches following the breach.

5.2 | Interviews

Semi-structured interviews then increased reliability and provided further validity to the findings (Morse 2010). The 12 industry experts (detailed in Table 3) participating in the interviews were selected using the following selection criteria:

1. Professionals engaged in TS management for at least 5 years.
2. Currently holding leading positions in Intellectual Property (IP) management OR from the top management of organizations that experienced TS misappropriation and were consequently involved in active litigation.

Interviews lasted between 30 and 60 min and used open-ended questions concerning mitigation of TS misappropriation. The participants were asked questions, such as "What is the process of TS misappropriation-mitigation in your organization?" Data saturation was reached after 7 interviews.

To analyse the interviews and the legal cases, NVivo was used, and thematic analysis followed an abductive approach described in Clarke et al. (2015), utilizing the framework presented in Figure 2, and the stages, adapted from Rojon et al. (2021), shown in Table 4. The DC theoretical framework in Figure 2 is therefore used to justify the processes focused upon, guide the analysis, and interpret the findings meaningfully.

The structural coding applied to establish code categories followed guidelines outlined by Saldaña (2021), and subsequent intercoder reliability procedures were implemented to define and label code themes in accordance with O'Connor and Joffe (2020). The thematic analysis process then further outlined in Table 4 allowed our study to identify the stages of TS misappropriation-mitigation and map out the measures organizations undertake upon acknowledging misappropriation. We were also able to design strategies for avoidance of TS misappropriation.

6 | Results

The findings are summarized in Figures 3 and 4 below. Results show that the TS misappropriation-mitigation process encapsulates the actions an organization can take to prevent its TSs from complete disclosure and loss. Figure 3 below demonstrates this step-by-step process.

TABLE 4 | Thematic analysis process of interviews (Adopted from Rojon et al. 2021).

Step	Action
1.	Selection of participants based on inclusion and exclusion criteria.
2.	Preparation of interview questions.
3.	Interview collection.
4.	Interview data consolidation.
5.	Familiarization with the interview data in NVIVO (Tranfield et al. 2003). Identification of initial themes in interview data (TS management process, protection).
6.	Structural coding and generation of initial codes from interview data (*TS management process, TS identification, TS audit*).
7.	Search and review of interview data themes in Nvivo.
8.	Use of intercoder reliability to define interview data themes in Nvivo (*TS misappropriation-mitigation stages; TS misappropriation-mitigation measures*).
9.	Consolidation and refining of the results.
10.	Writing up and presentation of findings

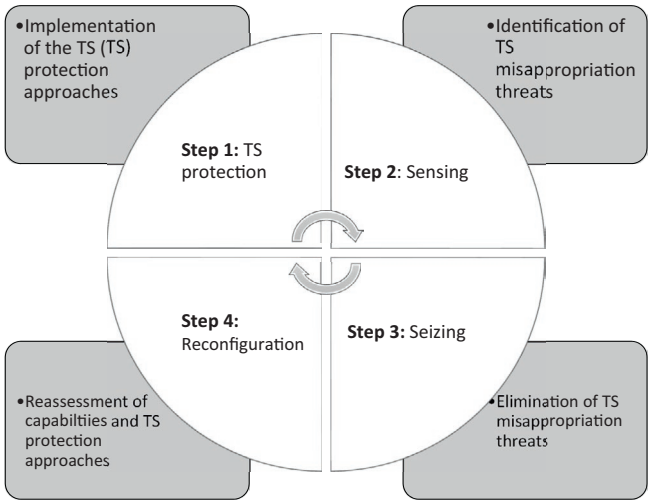

FIGURE 3 | The process of TS misappropriation-mitigation. [Color figure can be viewed at wileyonlinelibrary.com]

The process begins with TS protection approaches already in place within the organization. This allows the organization to achieve the highest efficiency from the mitigation process. Once the misappropriation threat has been identified, the company can follow specific strategies to maintain the TS and adjust itself in the event of a new misappropriation threat. This would entail strengthening the existing TS protection approaches or even a shift in business strategy. Figure 4 demonstrates all the identified strategies.

Figure 4 presents a more in-depth holistic overview of the TS misappropriation-mitigation process. It includes a detailed plan of action in the event of TS misappropriation. The flowchart is circular, the steps flow from step 1 to step 4 with redirection back to step 1. The following subsections explain Figure 4 in more detail.

6.1 | Step 1: Implementation of TS Protection

The TS misappropriation-mitigation process begins with the implementation of TS protection approaches within any given organization. In an ideal scenario, the presence of such approaches is determined by a recognized TS. This implies the TS is identified within the organization as valuable, rare, inimitable, and organized within the company, and specific protection approaches are put in place to safeguard such valuable and confidential knowledge (Ozcan et al. 2023). If the TS protection framework is absent, there is a potential for TS loss. The absence of TS protection approaches indicates the organization does not understand the concept of trade secrecy and does not assign commercial value to confidential information. The misappropriation-mitigation process cannot, therefore, begin without some TS protection approaches and measures available across the organization. In step 1, therefore, the TS protection framework needs to be examined to understand if the approaches and mechanisms are available and efficient.

Interviewees X11 and X6 argue that the efficiency of a protection framework defines the misappropriation-mitigation process. Efficiency in this regard is not determined by the absence of misappropriation instances. Instead, it is the capacity of the organization to identify strategically important valuable knowledge that is a TS or has the capacity to become one and protect it. The protection framework is then reinforced with multiple organizational approaches to maintain the secrecy of a TS (Ozcan et al. 2023; Bos et al. 2015).

According to the interviewees (X1, X3, X4, X10, etc.), establishing a TS protection framework entails understanding the IP, conducting an environmental assessment, and auditing valuable information. These steps enable organisations to determine which pieces of information they would like to maintain as TSs. All interviewees maintain that the TS protection framework needs to be designed according to TS requirements outlined in the 2018 Trade Secret Regulations. In simple terms, for the TS to be recognized as one in court, it is necessary to demonstrate that the information in question:

1. Possesses commercial value because of its secrecy;
2. Is limited in knowledge to a number of individuals; and
3. Is kept secret by a rightful owner through reasonable steps, such as confidentiality agreements or other means (European Union 2016; Trade Secrets Regulation, Article 2 2018; Ozcan et al. 2023).

The case law analysis demonstrates that the TS requirement test is the first step in TS litigation. Organizations that fail to fulfill these requirements lose their opportunity to mitigate damages resulting from misappropriation and receive any form of

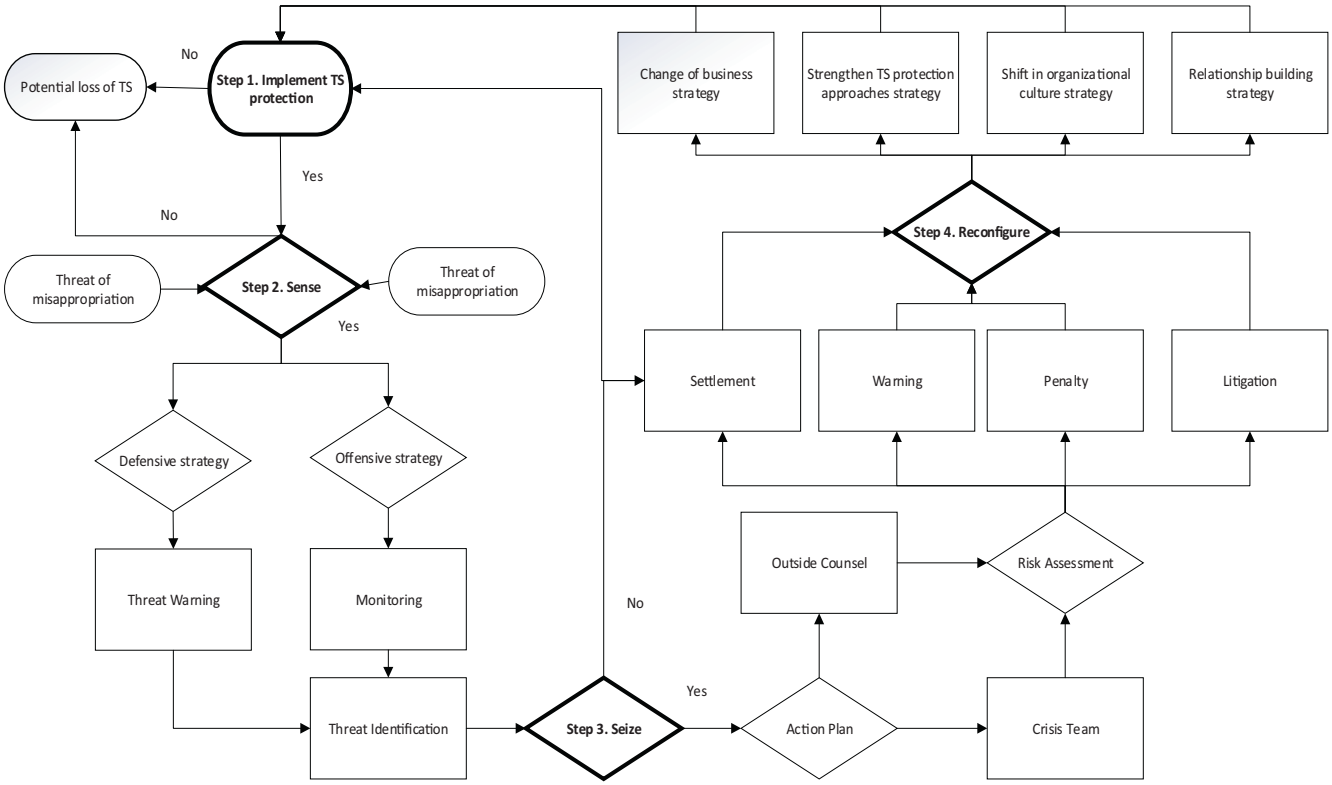

FIGURE 4 | The flowchart of TS misappropriation-mitigation. [Color figure can be viewed at wileyonlinelibrary.com]

compensation as a result of litigation (Invista Textiles (UK) Ltd v Botes 2019). To conclude, the existence of an up-to-date TS protection framework is an initial step and a requirement for a successful TS misappropriation-mitigation process.

6.2 | Step 2: Sensing TS Misappropriation

The research data plays a pivotal role in elucidating the principles of DC theory (Teece 2007), thereby laying a robust foundation for the subsequent discussion. It also significantly enriches our understanding of the sensing, seizing, and reconfiguring activities in the TS-specific context. Organizations are prompted to closely guard their valuable information in response to environmental changes such as employee mobility, changes in employee behaviour, and changes in suppliers. The sensing stage in the mitigation process is the period when the organization becomes aware of and alarmed by potential threats to their TSs, which can emanate from both within and outside the organization. Failure to act upon these threats to TS misappropriation can lead to potential TS loss.

According to the study's findings, detecting TS misappropriation can involve both offensive and defensive strategies. A defensive sensing strategy involves monitoring the activities of former employees or competitors through social media or other information channels. According to interviewee X2, "We are defensive, and it is hard to determine whether your IP has been stolen in my industry." X7 and X9 also agree that some industries, especially software, require a more toned-down approach to TS misappropriation observation. Most interviewees agree that this is due to the high litigation costs and the desire to maintain a non-aggressive reputation within the industry.

If a company wants to signal to competitors or other industry actors its seriousness about protecting its IP rights, an offensive mitigation strategy is employed. During an offensive sensing strategy, the companies engage in continuous, active, monitoring of all parties having access to its TS or with the capacity to access it (X3, X4, X10), including monitoring of patent activity, social media, AI-integrated network monitoring tools (email tracking, downloading activity tracking, etc.), and changes in working patterns, and so forth. (X1, X2, X4, X5, X6, X7, X10, X11). As interviewee X9 puts it, 'We follow a fortress approach, in a sense, and you have to have the tools to monitor, and people to use them.' This continuous monitoring is crucial for identifying keywords or utilizing our artificial intelligence to detect specific types of behavior.

The result of these defensive and/or offensive strategies is the identification of TS threats. Suppose the source and impact of the threat are identified and flagged in the IT system or by an employee. In that case, the company can tailor appropriate response actions that follow in the sensing part of the mitigation process (X5). In a defensive strategy, however, it may take longer to identify the threat, which can impede the secrecy and consequent value of a TS (Invista Textiles (UK) Ltd v Botes 2019).

6.3 | Step 3: Seizing of TS Misappropriation

Seizing then generates a response to an identified threat of TS misappropriation. Four types of response were identified in the seize stage: settlement, warning, penalty, and litigation. All the interviewees agree that avoiding litigation is the preferred

outcome in the event of TS misappropriation, with settlement, issuing a warning, or a penalty being the options to be pursued before litigation commences.

Once a misappropriation threat is identified, a swift response is crucial. As interviewee X9 emphasizes, "what you do in the first few minutes, the first few hours, or the first few days is critical." This prompt response is crucial to prevent the dissemination of information before it can be shared with others. It involves referring to the mitigation action plan, the prescriptive plan of action, and the initial steps the company should take in the event of TS misappropriation. While all interviewees acknowledge the importance of such an action plan, only a few had it available in the workplace (X4 and X12).

After the initial reaction, the companies either contact outside legal counsel, form a crisis team, or assign an individual to oversee all further actions in the mitigation process (X7, X8, X11). A risk assessment of the misappropriation threat then follows, to measure the potential damage from the TS misappropriation threat (Surdeanu et al. 2011). For example, according to interviewee X12, 'we made an assessment that, given the amount of time he was on site and who he was with, we decided he was at the lower end of the risk spectrum.' This process underscores the significance of relationship building and trust in the industry, as it facilitates a more precise risk assessment and accurate measurement of potential damage.

Once the risk is assessed, the company can pursue appropriate action. If the potential for TS disclosure is low, warnings and penalties for misconduct can be implemented, and HR tools can be utilized to intervene in the event of suspicious behaviour being identified (Hannah et al. 2019). Warnings can also be issued to employees, competitors, or suppliers to stop using the TS in question and return all the valuable information (ESL Fuels Ltd v Fletcher and Anor 2013; Norbrook Labs (GB) Ltd v Adair 2008).

Settlement is another possible venue for mitigating TS misappropriation. The organization approaches the party guilty of TS misappropriation with an option to cease the use of a TS and return all the documentation to the organization (Dyson vs Technology Ltd v Pellerey 2015; Invista Textiles (UK) Ltd v Botes 2019). This request can lead to either the settlement of TS misappropriation or litigation. According to the majority of interviewees, settlement and return of documentation are the preferred resolution options for the organisations involved. According to Borghi et al. (2023), on average, TS misappropriation disputes typically include employers and employees, and last between 2 and 4 years. Consequently, litigation is pursued as the avenue for TS misappropriation mitigation only in instances where settlement is not an option, such as when disclosure of a TS is required, reputational damage is incurred, or an inability to agree exists (Celgard v Shenzhen Senior Technology Material 2020).

It is the calculation of damage to the company based on the commercial value of the TS in question that compels an organization to initiate proceedings against the guilty party (Borghi et al. 2023). In some cases, the misappropriation of a trade secret (TS) constitutes a loss of competitive advantage for a company, and litigation becomes the only viable solution to recover losses and maintain business operations. Litigation offers various remedies for TS misappropriation, from injunction to compensation for damages.

For litigation to be effective, however, the party initiating the proceedings must demonstrate to the court evidence of a TS and its misappropriation by the defendant (Borghi et al. 2023). The party initiating proceedings must prove that the misappropriated information is indeed a TS, as defined by Article 2 of the EU Directive 2016/943 (European Union 2016). Additionally, however, interviewee X9 identifies the necessity to prove that the defendant possesses a TS due to misappropriation, rather than independent discovery. Failure to establish one of these requirements before the court can result in no relief or rejection of a breach claim altogether (FSS Travel v Johnson 1997; Caterpillar Logistics Services (UK) Ltd v Huesca de Crean 2011; FNM Corporation Ltd v Drammock International Ltd 2009). According to all the interviewees, new instances of TS misappropriation, cyber theft, and the introduction of the EU Directive 2016/943 (European Union 2016) on the protection of undisclosed know-how and business information (TSs) forced businesses to acknowledge the importance of information auditing and application of TS requirements to secure their intellectual property assets in the event of litigation.

6.4 | Step 4: Reconfiguration of TS

Our findings suggest that reconfiguration is the final stage of TS misappropriation-mitigation. In line with DC theory, reconfiguration entails realignment of operations as a result of changes in the environment (Teece 2007). The changes in the environment during the process of TS misappropriation-mitigation are the events that follow the sensing and seizing stages, after a threat to the company's TS or loss of it. The reconfiguration stage involves realigning and adjusting company processes to reflect the outcomes of TS misappropriation (Barreto 2010). Such realignment is conducted through strategic actions to improve companies' existing and new IP assets management to maintain competitive advantage. Our findings also identify four strategic actions that can be incorporated together or individually: relationship building, shifts in organizational culture, strengthening TS protection approaches, and changes in business strategy, outlined in the following sub-sections.

6.4.1 | Relationship Building Strategy

Relationship building is one of the strategies employed by organisations following the misappropriation or threat of misuse of a trade secret (TS). According to the majority of interviewees, building trusting relationships with employees and other stakeholders about TS protection is often overlooked. Understanding the importance of trust and good relationships typically arises after an incident of TS misappropriation, especially since employee mobility is one of the primary causes of TS misappropriation (Delerue and Lejeune 2011; Borghi et al. 2023).

Dissatisfaction with management, company strategy, or working conditions is among the most frequently cited reasons for theft of services (TS) misappropriation in TS litigation cases (Dorma UK Ltd v Bateman 2015; Extec Screens and Crushers Ltd v Rice 2007; Invista Textiles (UK) Ltd v Botes 2019). In the case of Allfiled UK Ltd v Eltis (2015), employees accused of misappropriation of a TS reported several serious disagreements with management regarding the fair share of equity participation. According to Hannah (2005), employees who do not feel trusted and/or appreciated are less likely to protect company TSs. Interviewees X2, X5, X10, and X11 maintain the same point of view. Forming and maintaining a positive professional relationship where employees are valued, rewarded, and respected is therefore key in avoiding TS misappropriation.

Interviewee X6 states that, following the period of redundancies after the TS litigation, the company adopted a new approach to stakeholder management. The new stakeholder management approach entailed building more trusting relationships with employees and suppliers that would preclude them from leaving the company or revealing the company's potentially valuable information. X11 maintains the same opinion and argues that stakeholder management built on trust also works even if employees or other stakeholders no longer have a relationship with the organization owning the TS. Trusted individuals and organizations are less likely to engage in TS misappropriation (Hannah 2006).

6.4.2 | Organizational Culture Shift Strategy

Changing to a culture of greater secrecy is another strategy employed by companies that have experienced or attempted TS misappropriation. Such a change entails a focus on continuous education, including master classes, videos, and quizzes, as well as staff retention. Training, onboarding, and positive offboarding are among the measures specified by the interviewees. According to interviewee X10, "You need to educate them on how it works [TS]." *Many of them do not realize that something is sensitive and has value to the company.*

Interviewee X7 stipulates that TS protection awareness training reduces the chances of future litigation and serves as evidence of "reasonable measures undertaken by organisations to protect the TS" in court (EU Directive 2016/943 European Union 2016). According to interviewee X7, much of the time, TS misappropriation is unintentional. Before someone accesses a TS, they must acknowledge that they know it is a TS. They will only do good things with it. The training goes a long way.

Re-evaluation of onboarding and offboarding procedures is also part of organizational culture changes. Onboarding changes involve the introduction of induction processes that focus on explaining intellectual property to new employees (X1, X2, X7, X9, X10, X11). The induction process also includes a reminder to new starters during entrance interviews of their obligations not to bring TSs from their previous employers (X7). We explain the internal processes to them and conduct frequent checks and early monitoring (X9, X11). The induction process is also there to remind newcomers not to bring TSs from their past companies.

According to interviewee X2, "*As part of the exit strategy, we have a proper discussion with the employee, so we do not pass our information to someone else. We ask them to sign a letter. We do not force them to sign this document, but the fact that they see it means we will take it seriously.* Most interviewees stipulate that in recent years more attention has been given to the development of offboarding practices. According to interviewees X1, X2, X5, X7, X10, and X11, the offboarding of a person with access to confidential information entails providing them with notice, a gardening leave, or a reminder of their obligations towards the organization. X2 and X3 argue that it is difficult to prevent knowledge from leaving the company, and there is a need to ensure that someone else in the organization can also take over that knowledge." Interviewee X11 emphasizes the importance of positive offboarding and the need to be cautious with bad leavers.

Finally, organizational culture adaptation can include a change in attitude towards organizational openness. Interviewee X7 argues, "*When it comes to TSs, you've to temper that openness a little bit. We do limit access, and it might mean that as our company grows, certain employees will not have access to certain TSs.*" Interviewee X3 also presses against organizational openness. This is especially relevant for SMEs and start-ups that tend to hire inexperienced workers. According to interviewee X3, "*they [new employees] come from an open environment, and they feel free to discuss what they are doing with anyone. It is essential to explain to those people the changes in the environment and the reasons behind them*". Consequently, according to interviewees X7 and X3, such actions require management initiative and consistency.

6.4.3 | Strengthening of the TS Protection Strategy

The threat of misappropriation or unauthorized access to a TS itself forces organizations to reassess their existing organizational TS protection approaches. X6, X4, and X2 noted that their prior experience with litigation over TS misappropriation had compelled their companies to reassess their protection approaches and adopt a more proactive protection strategy. Our findings suggest that each company employs a distinct approach to TS management. The common feature of TS protection strengthening, however, is an emphasis on the "*need-to-know*" approach to information access for employees across the organization.

According to all the interviewees, however, the initial step is to conduct a TS audit. Once all the valuable information is identified, it needs to be categorized by importance. Interviewees X1, X9, X10, and X12 specify a "cataloguing system," where all valuable information is labeled as "non-confidential," "confidential," and "TSs." A majority of the interviewees noted that a specific person or team needs to be assigned by management to oversee the processes and projects specific to each TS.

A more stringent approach to information management is also required. Interviewees X9 and X12 note that "security on documents and good contracts are also critical." X4 also mentions

information fragmentation as an approach developed within the organization following the TS litigation. Interviewee X7 employs a "gatekeeping process" where all information intended for public release undergoes an IP check. Finally, once the protection framework is reassessed, continuous monitoring and reminders of obligations to employees are prioritized. This is to maintain awareness of TS misappropriation threats that can arise in the future.

6.4.4 | Change in the Business Strategy

It is likely, however, that companies experiencing TS misappropriation can lose some of their competitive advantage (Al-Aali and Teece 2013). For some organisations, their TS can be the only means of securing their unique customer offering (ESL Fuels Ltd v Fletcher and Anor 2013). X6, X4, and X2 maintain that following a threat and the loss of a TS, companies undergo a period of uncertainty, which defines their future business operations.

In the case of ESL Fuels v Fletcher (2013), the company lost its TS and a key business partner to a competitor. ESL Fuels had to reassess its competitive advantage and develop a diversified product offering, targeting a range of new clients (ESL Fuels 2023). Unfortunately, there are also known instances where companies with a TS go out of business after TS misappropriation litigation (Ozcan et al. 2023).

Hence, interviewees X6, X4, and X2 maintain that acknowledging the potential impacts of TS misappropriation on the business's overall health is an initial step following the misappropriation threat. Reconfiguration and reassessment of the valuable resources and business partners is the second step in the business strategy overview following the misappropriation. It is vital to audit all valuable knowledge again, reassess existing TSs, or even identify new ones. According to interview X12, "we analysed every aspect of the company... we've set meetings, and we devised a plan to move forward." The plan to move forward also encapsulates the synergy between a business strategy and an IP strategy (Interviewees X7 and X12, 2023).

Finally, uncertainty is another underlying cause of employee TS misappropriation (*Caterpillar Logistics Services (UK) Ltd v Huesca de Crean*). In the case of Allfiled UK Ltd v Eltis (2015), the defendants complained of dysfunctional decision making. Therefore, coherent organizational governance can complement the synergy between a business and IP strategy development.

7 | Discussion

7.1 | Theoretical Contributions

Prior studies (Bos et al. 2015; Basuchoudhary and Searle 2019; Ozcan et al. 2023; Wang et al. 2023) have not explored the mitigation of TS management in light of RBV and DC theory stages. Because potential changes in the environment can impact TSs within the company, structured organizational efforts are necessary to maintain the secrecy of valuable information and sustain the organization's competitive advantage (Khan et al. 2021; Shiau et al. 2023). Our study presents a unique, evidence-driven, stage-by-stage approach to mitigating TS misappropriation, aligning with the sensing, seizing, and reconfiguration stages of DC theory (Teece 2007). This makes a theoretical contribution by integrating DC theory into the framework for trade secret misappropriation mitigation, and also, novelly, by providing details on what this means in practice, beyond the existing literature. This identifies what a DC approach looks like in the specific TS context, DC theory itself, helping to meet the criticisms of Collis et al. (2021), contextualizing DC in line with Gremme and Wohlgemuth (2017), concerning the impacts of contingency conditions (Barreto 2010), and differences in DC types within different strategic settings (Vu 2020).

Second, existing studies in the area of TS management mention mitigation as a final step of TS management (Maurer and Zugelder 2000; Bos et al. 2015; Wang 2021; Ozcan et al. 2023; Fedorenko et al. 2023). However, none explore the processes of TS misappropriation-mitigation in depth. Our study contributes to the literature on TS management by analyzing data drawn from the mistakes of organizations previously involved in TS litigation in the UK and interviewing key specialists in the area. Specifically, we were able to devise a coherent and comprehensive overview of the mitigation stages and approaches within them.

Third, existing research on TS management does not address the question of TS protection framework efficiency (Maurer and Zugelder 2000; Bos et al. 2015; Wang 2021; Ozcan et al. 2023). We identify that the presence of the TS protection framework within the organization does not guarantee the non-occurrence of TS misappropriation, but does identify a more efficient process, contributing to the overall literature on TS management.

7.2 | Practical Contributions

Our study also offers several practical contributions. First, our empirical analysis reveals that, as there is usually no accepted or coherent approach to misappropriation-mitigation established in firms in the UK owning TSs or valuable information, they tend to underestimate the importance of misappropriation-mitigation in TS management. Our study raises awareness regarding mitigation practices in such organizations.

Second, we offer a practical step-by-step framework for TS misappropriation-mitigation in organisations in the UK, building from RBV to DC theory and offering action steps in the event of TS misappropriation or misappropriation threat. Each action step offers a variety of approaches organizations can follow. Third, the study indicates the need for the development of an all-encompassing TS policy by government and organisations. The organizational policy needs to include all aspects of TS management: from audit of valuable information and TS identification to misappropriation-mitigation steps.

Fourth, we find top management in the UK often does not attend training on trade secrecy and lacks an understanding of the

boundaries of secrecy, especially during collaborative projects. Implementation of a TS protection framework and its policy in an organization is a top-down process, requiring managerial intent. Therefore, our study highlights the need for trade secrecy awareness on a managerial level.

Finally, we offer reconfiguration strategies to follow for organizations that have undergone TS misappropriation or TS misappropriation threats in the UK. Strategies include organizational culture shift, relationship building, strengthening of TS protection approaches, and changes in the overall business strategy. The strategies can be adjusted and chosen according to the organization's needs following the misappropriation incident.

8 | Conclusions

TS misappropriation necessitates a prompt response and effective mitigation measures. The results of our study demonstrate that the process of TS mitigation starts with a TS protection framework tailored for a specific TS. The process of TS misappropriation-mitigation in the UK consists of four distinct stages, adding an initial trade secrecy protection stage that then links with DC stages of sensing, seizing, and reconfiguring (Teece 2007). These TS misappropriation-mitigation stages entail a distinct set of mitigation approaches available for the organizations to address TS misappropriation. The final reconfiguration stage presents four strategies to prevent TS misappropriation and enhance TS misappropriation-mitigation in the future.

Our study highlights the importance of the process and the need for TS misappropriation-mitigation processes in organisations that own a TS. We have also established that the implementation of cohesive mitigation processes requires management awareness and action. This includes ongoing IP training for both employees and management, establishment of a TS policy, and frequent auditing of valuable information for TS identification.

9 | Limitations and the Need for Further Research

The study has limitations, suggesting the need for further research. Specifically, the area of TS management could benefit from further exploration of the initial stages of TS identification. This entails both the process and stages of TS identification. In this regard, the use of theories of mindfulness in motivating information configuring and processing and sharing (Awan et al. 2024) would also be of benefit. We also find that more research is needed in the area of TS auditing. Research needs to focus on identifying a TS and the subsequent intricacies of TS monitoring. Finally, establishing the TS protection framework and exploring all the stages of TS management in other industries and regions would also contribute to the area.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

Al-Aali, A. Y., and D. J. Teece. 2013. "Towards the (Strategic) Management of Intellectual Property: Retrospective and Prospective." *California Management Review* 55, no. 4: 15–30.

Andersen, B., and L. Striukova. 2010. "Where Value Resides in the Modern Enterprise." *Strategic Change* 19.

Awan, U., M. Sufyan, I. Ameer, S. Shamim, P. Akhtar, and N. U. Zia. 2024. "Mindfulness and Creative Process Engagement: The Mediating Role of Workplace Relational Systems." *Journal of Managerial Psychology* 39, no. 3: 241–263.

Barreto, I. 2010. "Dynamic Capabilities: A Review of Past Research and an Agenda for the Future." *Journal of Management* 36, no. 1: 256–280.

Basuchoudhary, A., and N. Searle. 2019. "Snatched Secrets: Cybercrime and Trade Secrets Modelling A Firm's Decision to Report A Theft of Trade Secrets." *Computers & Security* 87: 101591.

Borghi, M., A. Cogo, and B. Khan. 2023. "Trade Secrets Litigation Trends in the Eu."

Bos, B., T. L. J. Broekhuizen, and P. De Faria. 2015. "A Dynamic View on Secrecy Management." *Journal of Business Research* 68, no. 12: 2619–2627.

Braun, V., and V. Clarke. 2014. "What Can "Thematic Analysis" Offer Health and Wellbeing Researchers?" *International Journal of Qualitative Studies on Health and Well-Being* 9, no. 1: 26152.

Clarke, V., V. Braun, and N. Hayfield. 2015. "Thematic Analysis." *Qualitative Psychology: A Practical Guide to Research Methods* 3: 222–248.

Collis, D. J., B. N. Anand, and S. Field. 2021. "The Virtues and Limitations of Dynamic Capabilities." *Strategic Management Review* 2, no. 1: 47–78.

Crittenden, W. F., V. L. Crittenden, and A. Pierpont. 2015. "Trade Secrets: Managerial Guidance for Competitive Advantage." *Business Horizons* 58, no. 6: 607–613. https://doi.org/10.1016/j.bushor.2015.06.004.

Delerue, H., and A. Lejeune. 2011. "Managerial Secrecy and Intellectual Asset Protection in SMEs: The Role of Institutional Environment." *Journal of International Management* 17, no. 2: 130–142.

Diestre, L., F. Lumineau, and R. Durand. 2023. "Litigate or Let It Go? Multi-Market Contact and Ip Infringement-Litigation Dynamics." *Research Policy* 52, no. 6: 104784.

Epstein, M. A., and S. D. Levi. 1987. "Protecting Trade Secret Information: A Plan for Proactive Strategy." *Business Law* 43: 887.

Esl Fuels. 2023. "ESL Fuels." https://www.eslfuels.com/about/.

European Union. 2016. "Eu Directive 2016/943 on the Protection of Undisclosed Know-How and Business Information." https://eur-lex.europa.eu/eli/dir/2016/943/oj.

Fang, L. H., J. Lerner, and C. Wu. 2017. "Intellectual Property Rights Protection, Ownership, and Innovation: Evidence From China." *Review of Financial Studies* 30, no. 7: 2446–2477.

Fedorenko, I., P. Berthon, and L. Edelman. 2023. "Top Secret: Integrating 20 Years of Research on Secrecy." *Technovation* 123: 102691.

Gerle, A., and J. Varsányi. 1997. "Business Prospects and Proprietary Management of A Hungarian Small Enterprise." *Strategic Change* 6, no. 7: 407–416.

Gremme, K. M., and V. Wohlgemuth. 2017. "Dynamic Capabilities: A Systematic Literature Review of Theory and Practice." *European Journal of Management Issues* 25, no. 1: 30–35.

Hannah, D., M. Parent, L. Pitt, and P. Berthon. 2019. "Secrets and Knowledge Management Strategy: The Role of Secrecy Appropriation Mechanisms in Realizing Value From Firm Innovations." *Journal of Knowledge Management* 23, no. 2: 297–312.

Hannah, D. R. 2005. "Should I Keep A Secret? The Effects of Trade Secret Protection Procedures on Employees' Obligations to Protect Trade Secrets." *Organization Science* 16, no. 1: 71–84.

Hannah, D. R. 2006. "Keeping Trade Secrets Secret." *MIT Sloan Management Review* 47, no. 3: 17.

Hemphill, T. 2004. "The Strategic Management of Trade Secrets in Technology-Based Firms." *Technology Analysis & Strategic Management* 16, no. 4: 479–494.

Jogulu, U. D., and J. Pansiri. 2011. "Mixed Methods: A Research Design for Management Doctoral Dissertations." *Management Research Review* 34, no. 6: 687–701.

Khan, F., J. H. Kim, L. Mathiassen, and R. Moore. 2021. "Data Breach Management: An Integrated Risk Model." *Information & Management* 58, no. 1: 103392.

Maurer, S. D., and M. T. Zugelder. 2000. "Trade Secret Management in High Technology: A Legal Review and Research Agenda." *Journal of High Technology Management Research* 11, no. 2: 155–174.

McGuinness, T., and R. E. Morgan. 2000. "Strategy, Dynamic Capabilities, and Complex Science: Management Rhetoric vs. Reality." *Strategic Change* 9, no. 4: 209–220. https://doi.org/10.1002/1099-1697(200006/07)9:4<>3.0.CO;2-G.

Morse, J. M. 2010. "Simultaneous and Sequential Qualitative Mixed Method Designs." *Qualitative Inquiry* 16, no. 6: 483–491.

O'Connor, C., and H. Joffe. 2020. "Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines." *International Journal of Qualitative Methods* 19: 1609406919899220.

Ozcan, O., D. Pickernell, and P. Trott. 2023. "A Trade Secrets Framework and Strategic Approaches." *IEEE Transactions on Engineering Management Journal* 71: 10200–10216. https://doi.org/10.1109/Tem.2023.3285292.

Passman, P. 2014. "The Economic Impact of Trade Secret Theft, (Create. Org)."

Pittaway, L., M. Robertson, K. Munir, D. Denyer, and A. Neely. 2004. "Networking and Innovation: A Systematic Review of the Evidence." *International Journal of Management Reviews* 5, no. 3–4: 137–168.

Rojon, C., A. Okupe, and A. McDowall. 2021. "Utilization and Development of Systematic Reviews in Management Research: What Do we Know and Where Do we Go From Here?" *International Journal of Management Reviews* 23, no. 2: 191–223.

Saldaña, J. 2021. "The Coding Manual for Qualitative Researchers." 1–440.

Santiago, F. 2017. "Trade Secret Protection on Globalization Era." *European Research Studies Journal* 20, no. 4: 66–76. https://doi.org/10.35808/ersj/820.

Searle, N. 2021. "The Economic and Innovation Impacts of Trade Secrets." UK Intellectual Property Office Research Paper, (2021/01).

Shiau, W. L., X. Wang, and F. Zheng. 2023. "What are the Trend and Core Knowledge of Information Security? A Citation and Co-Citation Analysis." *Information & Management* 60, no. 3: 103774.

Surdeanu, M., R. Nallapati, G. Gregory, J. Walker, and C. D. Manning. 2011. *Risk Analysis For Intellectual Property Litigation*, 116–120. Proceedings of the 13th International Conference on Artificial Intelligence and Law.

Teece, D. J. 2007. "Explicating Dynamic Capabilities: The Nature and Micro Foundations of (Sustainable) Enterprise Performance." *Strategic Management Journal* 28, no. 13: 1319–1350. https://doi.org/10.1002/smj.640.

Teece, D. J. 2010. "Business Models, Business Strategy, and Innovation." *Long Range Planning* 43, no. 2–3: 172–194. https://doi.org/10.1016/j.lrp.2009.07.003.

The Trade Secrets Enforcement Regulation 2018. 2018. "https://www.legislation.gov.uk/uksi/2018/597/made the National Security Act 2023." https://www.legislation.gov.uk/ukpga/2023/32/section/2.

Tranfield, D., D. Denyer, and P. Smart. 2003. "Towards A Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review." *British Journal of Management* 14, no. 3: 207–222.

Vu, H. M. 2020. "A Review of Dynamic Capabilities, Innovation Capabilities, Entrepreneurial Capabilities, and Their Consequences." *Journal of Asian Finance, Economics and Business* 7, no. 8: 485–494. https://doi.org/10.13106/jafeb.2020.vol7.no8.485.

Wang, L., Y. Zhang, and Y. Yan. 2023. "Offensive Patent Litigation Strategic Choice: An Organizational Routine Perspective." *Technovation* 122: 102663.

Wang, R. 2021. "Information Asymmetry and the Inefficiency of Informal Strategies Within Employment Relationships." *Technological Forecasting and Social Change* 162: 120335.

Wipo. 2022. "Wipo Symposium on Trade Secrets and Innovation 2022." https://www.wipo.int/meetings/en/2022/symposium-trade-secrets.html.

Cited Cases

Allfiled UK Ltd v Eltis & Ors 2015 EWHC 1300 (Ch).

Caterpillar Logistics Services (UK) Ltd v Huesca De Crean. 2011. EWHC 3154 (QB).

Celgard, LLC v Shenzhen Senior Technology Material Co Ltd 2020 EWHC 2072 (Ch).

Dorma UK Ltd v Bateman & Ors 2015 EWHC 4142 (QB).

ESL Fuels Ltd v Fletcher & Anor 2013 EWHC 3726 (Ch).

Extec Screens & Crushers Ltd v Rice 2007 EWHC 1043 (QB).

FNM Corporation Ltd v Drammock International Ltd & Anor. 2009. EWHC 1294 (Pat).

FSS Travel & Leisure Systems Ltd v Johnson & Anor. 1997. EWCA Civ 2759.

Invista Textiles (UK) Ltd & Anor v Botes & Ors 2019 EWHC 58.

Norbrook Laboratories (GB) Ltd v Adair & Anor 2008 EWHC 978 (QB).