Comprendre la déclaration frauduleuse du travail en contextualisant la théorie de la motivation à la protection

Frank Goethals*

Lies Bouten*

* IESEG School of Management, Univ. Lille, CNRS, UMR 9221 - LEM- Lille Economie Management, F-59000 Lille, France

Résumé :

Nous avons mené une étude qualitative, basée sur des entretiens, dans un contexte de déclaration frauduleuse du travail, où des propriétaires de restaurants déclarent des ventes et des paiements aux employés inférieurs à la réalité. Lorsque ces pratiques sont détectées, elles sont sanctionnées. Notre objectif était de comprendre en profondeur pourquoi certains individus adoptent (ou n'adoptent pas) le comportement d'adaptation consistant à « limiter ou arrêter la déclaration frauduleuse » face à la menace des « sanctions liées à la déclaration frauduleuse ». La présente recherche s'appuie sur des entretiens qui ont révélé des raisons d'agir conformes à la théorie de la motivation à la protection (PMT), une théorie mobilisée pour comprendre l'adoption de comportements d'adaptation dans le domaine des SI. Cependant, d'autres parties des récits ont mis en évidence la nécessité de contextualiser la PMT. Bien que les entretiens aient confirmé que la PMT constitue un cadre pertinent pour comprendre les comportements d'adaptation, ils ont également révélé que la PMT n'accorde pas une attention suffisante à certains facteurs contextuels qui pourraient être importants dans l'étude des SI, en particulier les menaces connexes et les comportements d'adaptation connexes. Cette étude examine les limites des conditions sous lesquelles la PMT s'applique, ce qui est directement pertinent pour la recherche en SI. L'interaction entre l'exploration des limites de la PMT et l'analyse des récits d'entretiens a conduit au développement du Cadre d'Évaluation des Menaces Connexes et des Comportements d'Adaptation Connexes (*Related Threat and Coping Appraisals Framework*, RTCAF). Ce cadre peut être utilisé par les praticiens pour concevoir des stratégies qui encouragent les individus à adopter des comportements d'adaptation spécifiques.

Mots clés :

Théorie de la Motivation à la Protection, conditions limites, comportement d'adaptation alternatif, menaces complémentaires, menaces concurrentes

Understanding work misrepresentation by contextualizing Protection Motivation Theory

Frank Goethals*

Lies Bouten*

* IESEG School of Management, Univ. Lille, CNRS, UMR 9221 - LEM- Lille Economie Management, F-59000 Lille, France

Abstract

We conducted an interview-based study in a work misrepresentation setting, where restaurant owners may register fewer sales and lower payments to employees than the actual sales and payments. If detected, such practices are penalized with sanctions. To gain a profound understanding of why actors may refrain from adopting the focal coping behaviour – limiting or stopping misrepresentation – when faced with the threat of such sanctions, the current research relies on interviews, which revealed rationales that aligned with Protection Motivation Theory (PMT), a theory frequently used to explain coping behaviour adoption in information systems studies. The narratives also suggested the need to contextualize PMT. While PMT offers valuable insights into coping behaviour adoption, it may also overlook critical contextual factors, including threats and coping behaviours that relate to the focal ones. The interplay between PMT's boundary conditions and interview insights suggests a novel framework, the Related Threat and Coping Appraisals Framework (RTCAF), that practitioners can leverage to design controls that encourage specific coping behaviours. In addition, by exploring PMT's boundary conditions, this article is directly relevant for IS researchers.

Keywords

Protection Motivation Theory (PMT), boundary conditions, alternative coping behaviour, complementary threats, competing threats

1. Introduction

Many information systems (IS) attempt to support traceability. Blockchains are implemented to establish reliable product traces, and technologies such as RFID-tags (Radio Frequency Identification-tags) are used to create digital twins, which are defined as "*a digital representation of any characteristics of a real entity, including human beings*" (Dambrot et al., 2018, p. 162). IS are often meant to represent states and state changes in the physical world, with the goal of obtaining reliable representations. Achieving accurate representation is regarded as the "*essence of*" IS (Weber, 2003, p. viii). "*By observing the behavior of an information system, we obviate the need to observe the behavior of the system it represents*" provided the IS "*enable 'faithful' tracking of other systems*" (Weber, 2003, p. viii). However, even the best designed IS fail to represent reality accurately when users falsify information. Real-world examples refer to cyclists switching identification chips to help a teammate qualify for a race championship (Huyberechts, 2024), as well as sales representatives manipulating sales figures to enhance their apparent performance and reputation within the company (Vieira da Cunha, 2013).

There are many cases of misrepresentation and these often boil down to fraud. In this study we undertake an in-depth investigation of what drives the decision to (not) misrepresent work in a specific industry setting. For many years, misrepresentation had been an issue in the Belgian restaurant sector. In particular, two work misrepresentation practices were salient in this context: (1) registering that employees work fewer hours than they actually do and (2) registering fewer sales than is true. These two forms of misrepresentation are closely linked. The first implies that employees' hidden hours are being paid unofficially, or under the table, and such payments require money that is not in the books. That is, the restaurant might conceal sales so it has unrecorded funds to pay employees for their unregistered working hours (Ainsworth & Hengartner, 2009). Accordingly, we define the term *work misrepresentation* to encompass both forms.

Work misrepresentation causes financial losses for the government, which relies on social contributions and taxes. Therefore, auditors working for the Belgian government are verifying whether such misrepresentation is taking place, and sanction restaurant owners engaged in these practices. Numbers related to these audits are available for Flanders, the northern part of Belgium, where we conducted our study. On a yearly basis, circa 6% of Flemish hospitality businesses undergo a labour audit (numbers on

tax audits are not disclosed)[1]. Penalties for both tax and social fraud can include substantial fines (e.g., fines going up to 200% of the avoided tax amount) as well as prison sentences. Despite the threat of these sanctions, restaurant owners have been misrepresenting working hours and sales for a long time. In 2021 for example, auditors found that 53% of inspected hospitality businesses were operating illegally (Matyn, 2022). Thus, the threat of sanctions appears to have been insufficient to motivate restaurant managers to represent working hours and sales correctly.

Sanctions represent just one type of threat studied in the IS domain. Many experimental IS studies have shown that threats - like password theft, malware infections, hard disk damage, identity theft, privacy risks and punishments for violating information security policies - may motivate individuals (e.g., citizens, employees) to adopt a coping behaviour (i.e., protection behaviour), in particular the focal coping behaviour included in the fear appeal provided to the participants. But the threat of sanctions appears insufficient to stop Belgian restaurant owners from misrepresenting working hours and sales, even though that focal coping behaviour is the one suggested in the fear appeal that the government creates. Therefore, we address our main research question, *why may actors refrain from adopting a focal coping behaviour in the presence of a threat*, in the context of the Belgian restaurant industry. Our interviews took place during an interesting period as the Belgian government had announced the requirement for restaurants to start using a Registered Cash Register (RCR), a cash register that does *not* afford a capability to erase revenues without that erasure being visible.

To gain in-depth insights into why people do or do not adopt a specific coping behaviour when faced with threats, we conducted an interview-based study, which also represents a response to Lee et al.'s (2008) call for qualitative research into the motivations for adopting protection behaviours. Specifically, we conducted 35 interviews with restaurant owners, employees, civil servants, an industry representative, cash register vendors, and accountants. In analysing the narratives provided during these interviews, we noted their resonance with Protection Motivation Theory (PMT; Rogers, 1975, 1983),

[1] https://guidea.incijfers.be/mosaic/dashboard1/gewestrapport-horeca; https://www.siod.belgie.be/nl/publicaties/statistieken

one of the most used theories in behavioral IS security studies. According to PMT, appraisals of a focal threat (in casu: misrepresentation sanctions) and a focal coping behaviour that might mitigate the threat (in casu: limiting or stopping misrepresentation) influence the decision to adopt the focal behaviour or not. Our qualitative findings affirm that both appraisals are part of restaurant managers' cognitive processes. Yet they cannot fully explain managers' intentions to limit (i.e., to lower) or stop their work misrepresentation. Therefore, this study establishes when threat and coping appraisals, as described in PMT, may not sufficiently explain the adoption of specific coping behaviours in the IS domain. We accordingly identify some relevant boundary conditions of PMT in the IS domain. Because the interview findings suggest the need to contextualize PMT (Hong et al., 2014), we develop a novel Related Threat and Coping Appraisals Framework (RTCAF) as a foundation for gaining a more accurate understanding of the adoption of coping behaviour in specific conditions present in diverse IS settings.

We review PMT literature in the next section, then describe the qualitative research setting and research method, with particular attention to our data analysis approach. The findings reveal when insights into focal threat and coping appraisals cannot provide a profound understanding of managers' decisions to adopt focal coping behaviours. In the discussion section, we present the RTCAF, detail our contextualization approach, link the findings to prior literature, outline PMT's boundary conditions, and address both implications and limitations of our study.

2. Literature review

The impact of threats on behaviour has received ample attention in the IS domain. When faced with threats, people seek to control their fear or the danger itself (Leventhal, 1970). According to the Extended Parallel Process Model (Witte, 1992, 1994), a danger control process seeks to mitigate the threat by adopting adaptive coping behaviour; a fear control process instead aims to reduce the sense of fear, without altering the danger, through the adoption of 'maladaptive coping behaviour' (e.g., wishful thinking) (Rippetoe & Rogers, 1987). Noting the frequency with which our interview participants cited the danger control process, we only seek insights into this process. Parts of our interview narratives read like a script of PMT, which initially was introduced to explain danger control processes, as depicted in Figure 1.

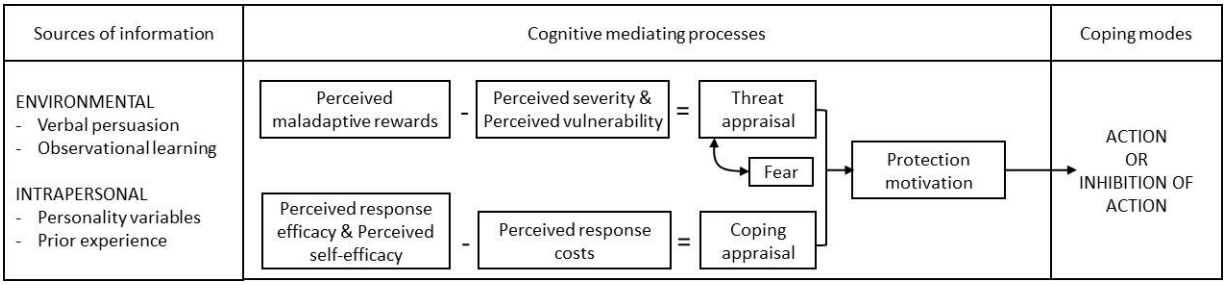

Figure 1: PMT (adapted from Rogers, 1983, p. 168)

PMT posits that people undergo cognitive appraisal processes in response to threats (Rogers, 1983), and those processes might be primary or secondary (Lazarus, 1991). The primary appraisal process centers on the threat; according to PMT, three factors produce a threat appraisal: perceived vulnerability, perceived severity, and perceived maladaptive rewards. Whereas perceived maladaptive rewards lower appraisals of the threat, perceived vulnerability and perceived severity increase it. If they identify a real threat, people then initiate a secondary appraisal, focused on coping (Floyd et al., 2000). In this process too, PMT identifies three appraisal determinants: perceived response efficacy, perceived self-efficacy, and perceived response costs. Both perceived response efficacy and perceived self-efficacy positively influence coping appraisals, but perceived response costs lower it. The result is a specific protection motivation, or behavioural intention, for adopting the focal coping behaviour. Although all these core PMT determinants, as defined in Table 1, reflect *perceptions*, we elide this term hereafter for brevity. Furthermore, for clarity, we define the threat of misrepresentation sanctions in our study context as the focal threat, and limiting or stopping work misrepresentation represents the focal coping behaviour.

Figure 1 also includes 'fear'. Some IS studies suggest that fear mediates the relation between threat and protection motivation (Lowry et al., 2023). However, in PMT, the emphasis was on protection motivation rather than fear to emphasize the importance of cognitive rather than visceral processes (Rogers, 1983). Rogers and Prentice-Dunn (1997) state fear has only an indirect impact, through severity appraisals; Siponen et al. (2024) even assert that fear is not critical to PMT. Therefore, we do not discuss fear further.

Perceived vulnerability	"*How personally susceptible an individual feels to the communicated threat*" (Milne et al., 2000, p. 108).
Perceived severity	"*How serious the individual believes that the threat would be to his or her own life*" (Milne et al., 2000, p. 108).

Perceived maladaptive rewards	Rewards associated with risky behaviours (Rippetoe & Rogers, 1987; Rogers, 1983).
Threat appraisal	The process of considering vulnerability to and severity of a threat, versus the maladaptive rewards associated with a behaviour that evokes the threat (Boss et al., 2015; Floyd et al., 2000; Rogers & Prentice-Dunn, 1997).
Perceived response efficacy	"*The belief that the adaptive [coping] response will work, that taking the protective action will be effective in protecting the self or others*" (Floyd et al., 2000, p. 411).
Perceived self-efficacy	"*An individual's beliefs about whether he or she is able to perform the recommended coping response*" (Milne et al., 2000, p. 109).
Perceived response costs	"*Any costs (e.g., monetary, time, effort, inconvenience, unpleasantness, difficulty, complexity, side effects) associated with taking the adaptive coping response*" (Lee & Larsen, 2009, p. 179).
Coping appraisal	A process of comparing self-efficacy and response efficacy with the costs of performing the coping behaviour (Boss et al., 2015; Floyd et al., 2000; Rogers & Prentice-Dunn, 1997).

Table 1: PMT core constructs

In addition to theorizing about threat and coping appraisals, PMT identifies two sources that can inform these appraisals: environmental sources (observational learning and verbal persuasion, including fear appeals) and intrapersonal sources (personality variables and prior experiences) (Rogers, 1983). Considerations of fear appeals dominated PMT research. Fear appeals "*are persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends*" (Witte, 1992, p. 329). A fear appeal contains descriptions of both a threat and a recommended coping behaviour (Boss et al., 2015; Rogers, 1983). Yet even as studies still pay significant attention to how fear appeals can trigger behavioural changes (e.g., Vance et al., 2022), PMT "*has moved beyond fear appeals and persuasion. The theory is now sufficiently broad to apply to any situation involving threat*" (Rogers, 1983, p. 172).

Thus, IS research has applied PMT to understand employee and citizen coping behaviours adopted to mitigate threats in work and private settings. In work contexts, such research has addressed behaviours such as cloud-based data backups (Menard et al., 2014), anti-spyware software use (Johnston & Warkentin, 2010; Liang & Xue, 2010), and anti-plagiarism software use (Lee, 2011), as well as reactions to threats linked to introduction of AI systems (Lysyakov & Viswanathan, 2023) and CEOs' protective and supportive actions (Barlette & Jaouen, 2019). Among citizens, PMT similarly has been applied to

understand anti-malware protection behaviours (Berthevas, 2021), anti-spyware software use (Gurung et al., 2009), and backup behaviour (Boss et al., 2015), along with diminished problematic smartphone gaming behaviour (Chen et al., 2020) and the use of wireless network security measures (Woon et al., 2005). Such applications involve both settings with specific threats (e.g., USB memory card theft) and specific coping behaviours (e.g., encrypting data on USB memory cards; Johnston et al., 2015) and those that feature more general threats (e.g., information security breaches in general) and general coping behaviours (e.g., complying with an information security policy; Herath & Rao, 2009). According to Schuetz et al. (2020), concrete fear appeals are more effective than abstract fear appeals. Referring to information security policy compliance, Aurigemma and Mattson (2019) argue that, rather than investigating compliance at the general level of the entire security policy, it may be better to investigate specific security actions, because each threat-specific security response might require a unique explanatory model.

As this widespread application indicates, PMT is a valuable theoretical lens. Yet several studies have failed to find significant relations between the core PMT constructs and coping behaviour adoption (Crossler et al., 2014; Tsai et al., 2016; Zhang & McDowell, 2009). Furthermore, some studies reveal significant relationships opposite to those predicted by PMT (e.g., Boss et al., 2015; Doane et al., 2016; Ifinedo, 2012; Vance et al., 2012). That is, prior PMT studies offer some inconsistent and inconclusive findings (Mou et al., 2022; Ng et al., 2021). To comprehend these inconsistencies in IS-PMT studies, we undertook an interview-based study. Qualitative studies are rare in this domain (Lee et al., 2008), but they may enhance understanding of why actors might adopt protection behaviours.

3. Research setting

Work misrepresentation through IS in the Belgian restaurant sector takes two forms, as we noted previously: misrepresenting employees' working hours and misrepresenting sales. To report employees' working hours, Belgian restaurant managers are obliged to use the Dimona information system, which affords managers the capability to register employees' hours and affords both managers and the government the capability to retrieve these registered data. Social security institutions retrieve Dimona data to calculate each employer's and employee's required contributions for healthcare, pensions,

unemployment, and so forth. In addition, government agencies use data retrieved from Dimona to check for compliance with labour laws (e.g., mandatory breaks, maximum working hours).

To register sales, restaurant owners historically had substantial freedom. They could choose their preferred cash register system, which afforded them to register, change, and delete orders, as well as process payments, and afforded them and the government the capability to retrieve these registered data. Depending on the type of restaurant and chosen cash register system, it provided other affordances as well, such as a capability to manage table reservations. Sales revenues entered into the cash register system enter accounting records and thus determine tax amounts and the amount of VAT remitted. Yet in addition, it has been relatively easy for restaurant managers to enter only some orders in their cash register system, using easy-to-destroy paper notes for others. Another way to hide sales relied on technologies, such as add-on zappers and factory-installed phantom-ware in electronic cash registers (Ainsworth & Hengartner, 2009) that make it easier to disguise sales. Such IS afford managers the capability to skim cash at the point of sale by deleting sales records, renumber receipts to disguise the deletion, and produce conforming financial reports. That is, such systems afford managers the capability to delete sales figures without the deletion being visible to others. While the IS afford managers the capability to register data that represent reality, managers often decide not to actualize the affordances and to misrepresent work instead. As we noted, misrepresenting employees' working hours requires misrepresenting sales too, implying overall *work misrepresentation* that creates relevant costs for the government. Sales misrepresentation causes the government to lose VAT and tax revenues. Furthermore, in Belgium, people with insufficient incomes often receive state benefits, and employees who officially only work part-time (but also are paid under the table) might appear to qualify for such benefits (Ainsworth & Hengartner 2009).

The Belgian government has threatened heavy sanctions for work misrepresentation. In PMT terminology, those sanctions constitute a threat (Johnston et al., 2015). Even in the face of this threat, around half of the audited restaurants have been caught engaging in work misrepresentation over the past ten years, solidifying the hospitality sector's reputation as one of the most fraudulent sectors (Matyn, 2022). This paper investigates why there was work misrepresentation despite this sanctioning

threat and will discuss other threats (than the misrepresentation sanctions) and other behaviours that may influence the work misrepresentation decision.

Our interviews reflect a particularly interesting stage, because the Belgian government had announced its goal to eliminate the previously common use of zappers and phantom-ware, available through freely chosen cash register systems, by requiring restaurants to start using a specific type of Registered Cash Register (RCR). Vendors offer hundreds of different RCR systems, but all of them share a notable characteristic: They do *not* afford a capability to erase revenues without that erasure being visible. Every sale entered in every RCR is stored, changes are recorded, and data cannot be deleted without leaving traces. In addition to this requirement, government agencies, together with the Flemish hospitality sector federation, issued fear appeal messages. The messages threatened misrepresentation sanctions; suggested, as a recommended coping behaviour, that managers stop misrepresenting; and implied that the RCR systems would render work misrepresentations impossible. They also emphasized elements of the new regulation, like allowing more overtime and lowering employer taxes on overtime pay, to enable restaurant managers to stop misrepresenting.

4. Research method

The decision by restaurant managers to adopt (or not) the focal coping behaviour of limiting or stopping their misrepresentation, in the presence of the threat of misrepresentation sanctions, largely takes place in each person's mind. Therefore, we turned to semi-structured interviews to capture the managers' rationales (Silverman, 2000). More specifically, the interviews provided insights into interviewees' perceptions, explanations and expectations. Then, to develop nuanced theoretical explanations for why people might adopt or refrain from adopting the focal coping behaviour, we applied an abductive research process, moving back and forth between the empirical evidence and our theoretical knowledge. Abduction is accepted as an integral part of interpretive research (e.g., Alvesson & Kärreman, 2007; Danermark et al., 2019; Gioia et al., 2013) and is widely embraced by proponents of critical realism. In this view, researchers must transcend the dualism between positivism and social constructivism and focus on understanding and explaining *why* things are as they are, by unravelling generative mechanisms

through a combination of data analysis, theory testing, and interpretation (Danermark et al., 2019; Mingers, 2004).

In the following sections, after describing the interviewees and selection process, we outline the interview process and how our questions sought to discover all elements that restaurant managers factor into their decision-making process as well as how these elements shape their decision-making. Finally, we explain how we analysed the interview data, why we mobilized PMT as an analytical tool to make sense of the interviewees' experiences, and how an abductive approach enabled us to "contextualize" PMT (Hong et al., 2014) and refine some of its concepts, as well as reveal generative mechanisms that typically are not considered in PMT.

4.1 Selection of interviewees

We interviewed 21 restaurant managers (including caterers), called 'managers' henceforth (see Table 2). The interviews revealed that other stakeholders influenced their perceptions and decision-making processes. Therefore, we also interviewed 14 such stakeholders (i.e., restaurant employees, civil servants in top positions, the CEO of the restaurant sector federation, cash register vendors, and accountants) (see Table 3). We used the insights from the latter interviews to establish a critical perspective on managers' views and find deeper meaning in their narratives (Klein & Myers, 1999). All the interviews took place in the year before the RCR was made mandatory, so managers were thinking about how they would need to change their organization to comply with the mandate. Two restaurants in the sample had already installed RCRs (RESB and RESN), and several others were close to installing them. All the restaurants were located in the same Belgian region, which enabled us to better grasp local stakeholders' impacts on managers' decision-making processes.

To develop a comprehensive understanding of managers' decision-making processes, we purposefully sought restaurants with different characteristics (e.g., opening hours, number of employees, price, cuisine). As work misrepresentation is illegal, we visited or called managers and employees in person to request interviews. In addition, we tried to reduce any potential social desirability bias in several ways. First, we promised to treat the interview data confidentially. Second, before the start of each interview, we emphasized that there were no right or wrong answers and that our aim was only to

understand the interviewees' decision-making processes, not to form any kind of judgment about it. Third, before we zoomed in on their decision-making, we invited them to share their perceptions of decision-making by *other managers or employees*. This approach could help them feel more comfortable discussing their own decision-making. Fourth, to build trust, we conducted the interviews face-to-face, in a regional dialect. Two contextual elements also alleviated the risk of social desirability bias. The restaurant sector federation had publicly acknowledged the prevalence of work misrepresentation, so though illegal, the practice is not a secret. In Belgium tax fraud was often regarded as almost a national sport (Van de Perre, 2014).

To solicit interviews with civil servants, sector representatives, cash register vendors, and accountants, we emailed reassurances that we would keep all information confidential. Although the interviews addressed sensitive topics, we sensed that all respondents talked openly.

Restaurant Abbreviation	Role & gender interviewees	Size	Age	Duration (min.)
RESA	Owner: M	M	O	75
RESB	Owner: M	L	O	70
RESC	Owner: M	L	O	60
RESD	Owner: M	S	O	80
RESE	Owner: M	L	O	55
RESF	Owner: M	L	O	115
RESG	Owner RESG1: F Owner RESG2: M Owner RESG3: F [1 interview with all interviewees together]	L	O	75
RESH	Owner: F	L	O	90
RESI	Owner: F	S	Y	30
RESJ	Owner: M	L	O	80
RESK	Owner: F	S	Y	15
RESL	Owner: M	M	Y	40
RESM	Owner: F	M	O	60
RESN	Owner RESN1: M Operational Manager RESN2: F Financial Manager RESN3: M [1 interview with all interviewees together]	M	O	65
RESO	Owner: M	L	Y	60
RESP	Owner: M	S	O	70
RESQ	Owner: M	M	Y	30

Table 2: Overview of interviews with restaurant managers: Gender (M: male, F: female), Size (S: <75 daily guests, M: 75-150 daily guests, L: >150 daily guests), Age (O: >5 years, Y: <=5 years)

Category	Abbreviation	Duration (min.)
Employees (6)	EMPA (employee of RESA)	70
From 5 restaurants	EMPB (employee of RESB)	10
	EMPE (employee of RESE)	20
	EMPJ1, EMPJ2 (both employees of RESJ)	60
	EMPX (employed by restaurant not in the sample)	30
Civil servants (2)	CS1 (civil servant, secretary of state for social fraud)	90
	CS2 (civil servant, tax auditor, heavily involved in RCR implementation)	120
Sector representative (1)	SR1 (CEO big sector federation in Belgium)	60
Cash register vendors (2)	CRV1	100
	CRV2	80
Accountants (3)	ACC1	90
	ACC2	60
	ACC3	50

Table 3: Overview of interviews (non-restaurant managers)

4.2 Conducting the interviews

The face-to-face interviews were conducted by both researchers, with the exception of CRV1, interviewed face-to-face by one researcher. Interviews were semi-structured to invite interviewees to participate in a guided conversation (Patton, 2002). The initial protocol included broad questions focused on why managers did (or did not) correctly represent work, how they designed managerial processes to support their (mis)representation, and whether the RCR implementation seemed likely to alter their answers to these questions. Interview guides can be found online as supplementary materials.

After transcribing some interviews, we recognized that the narratives of the restaurant managers often read like scripts of PMT. The PMT lens thus emerged from the data. Furthermore, our initial analyses indicated that, beyond the focal threat and focal coping appraisals, interviewees also mentioned contextual factors that affected their intentions to limit or stop misrepresentation (e.g., worries about recruiting employees), which could lead to outcomes contradictory with the patterns suggested by PMT. To gain a deeper understanding of the impacts of contextual factors, we slightly amended the interview guide during the interview phase (Patton, 2002; Silverman, 2000). For instance, we extended questions

about how stakeholders shaped decision-making by managers. We also actively searched other elements that might influence managers' misrepresentation decisions and asked for examples when they cited such elements. Because such contextual elements were raised organically by the managers, they must have been relevant; the personal relevance of threats is a condition for the applicability of PMT (Lowry et al., 2023). Yet we explicitly did not redesign or rebuild our interview guide around PMT, for two reasons. First, we wanted to continue exploring the possibility that other theoretical lenses could (also) help us make sense of the data. Second, integrating PMT constructs into the interview guide could have put ideas into interviewees' minds, and we wanted to avoid such influence. We sought *their* meanings and views. That is, the revised guide for later interviews differed only slightly from the initial guide.

Before each interview, we explained our research project, emphasized that there were no right or wrong answers, and encouraged respondents to speak freely. All but three interviewees (EMPB, RESH, RESP) gave permission for the interviews to be recorded. We also took detailed notes during and immediately after all interviews. Furthermore, we transcribed all recorded interviews verbatim immediately after they ended, which helped us become immersed in the data (Patton, 2002). The transcripts were analysed in the original interview language; the native language of the interviewers and interviewees. Only the quotes presented in the findings section were translated into English.

4.3 Data analysis approach

Our systematic data analysis involved data reduction, display, and interpretation (Miles et al., 2020). During our iterative coding, we made progressive adjustments on the basis of our data display and interpretation efforts (Sarker et al., 2013). The coding spanned three rounds. To avoid bias, both researchers engaged independently in each coding round, then discussed and compared results before registering the final coding outcomes using NVivo.

In the first round, which largely overlapped with our data collection, we mainly engaged in descriptive and *in vivo* coding (Saldaña, 2013). It generated an enormous number of codes, so we started to search for patterns and theoretical frameworks that could guide our continued search. For example, we considered Laughlin's (1991) organizational change framework and magic bullet theory (Markus & Benjamin, 1997) as potential theoretical lenses. Following several data–theory iterations, we recognized

that many codes pertained to threat and coping appraisals that played a role in the decision to (not) misrepresent work. In addition, some of the codes we had registered mentioned elements that explained why these appraisals did often not engender a decision to stop misrepresenting work.

In a second coding round, we linked narratives that referred to appraisals of the focal threat and focal coping behaviour to core PMT constructs. Building on the interpretations we gathered in the first coding round, we also grouped some codes into contextual factors that we labelled as related threats (e.g., "finding no employees") and related coping behaviours (e.g., "participate in alert network"). By reflecting on how these factors influenced restaurants managers' decision-making, we realized they could be regarded as boundary conditions of PMT (Hong et al., 2014). Boundary conditions are temporal and contextual factors that "*place limitations on the propositions generated from a theoretical model*" (Whetten, 1989, p. 492); they influence a theory's accuracy and generalizability across empirical contexts. To identify and refine the boundary conditions on PMT - which have not been delineated in prior literature, to the best of our knowledge - we began iterating back and forth between extant literature and our empirical findings.

Therefore, we embarked on a third coding round to reveal relevant contextual conditions and interpret their impacts (Busse et al., 2017; Whetten, 2009). In detail, we considered alternative coping behaviours, complementary threats, competing threats, additional benefits, and the legitimacy of coping behaviours. Table 3 outlines which contextual conditions were mentioned in relation to each of the restaurants in our sample. Overall, these PMT contextualization efforts, which build on Busse et al. (2017) and Hong et al. (2014), led us to introduce refinements to PMT concepts and incorporate additional generative mechanisms, in the form of the proposed Related Threat and Coping Appraisals Framework (RTCAF).

	Alternative coping behaviours	Complementary threats	Competing threats	Additional benefits	Legitimacy of coping behaviour
RESA	x		x	x	x
RESB	x	x	x		x
RESC	x	x	x	x	x
RESD	x	x	x		x
RESE	x	x	x		x
RESF	x	x	x	x	x
RESG	x	x	x	x	x
RESH	x		x		x

RESI		x			x
RESJ	x	x	x		x
RESK		x			
RESL		x	x	x	x
RESM	x		x	x	x
RESN	x		x		x
RESO		x	x		x
RESP	x				
RESQ	x			x	

Table 4: Managers' mentions of contextual conditions during interviews

5. Findings

In this section, we outline managers' decision-making related to work misrepresentation prior to the RCR introduction, then detail how its introduction influenced their decision-making processes.

5.1 Prior to RCR introduction

The interview narratives clearly indicate that managers actively appraise both the focal threat of misrepresentation sanctions and the focal coping behaviour of limiting or stopping misrepresentation. In addition, their narratives reveal other contextual factors impact the decision-making process. This section documents the narratives about the focal threat and coping appraisals and other contextual factors and illustrates clear insights into the influences of these factors are needed to gain a comprehensive understanding of managers' decision-making about the (mis)representation of working hours and sales.

5.1.1 Managers' appraisals of the focal threat and focal coping behaviour

The interview narratives reveal that when managers appraise misrepresentation sanctions, they consider their vulnerability to this focal threat and how severe it would be if it occurs, as well as the rewards associated with not attempting to avoid the threat. That is, they engage with PMT's threat appraisal constructs. Then, when appraising limiting or stopping misrepresentation, managers reflect on the response efficacy of this focal coping behaviour, their self-efficacy, and the associated response costs. In Figure 2, we demonstrate how the core PMT constructs arise in our research setting.

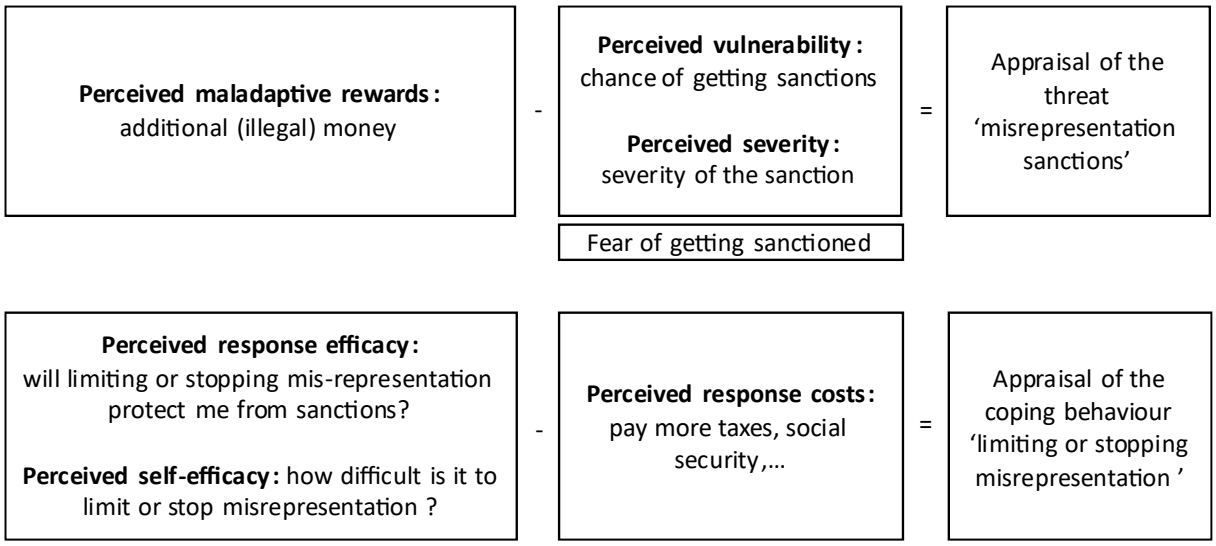

Figure 2: Core PMT constructs applied to our setting

5.1.1.1 Appraisal of the threat 'misrepresentation sanctions'

Restaurants can be sanctioned for misrepresenting work. These sanctions are considered a *threat* by managers (Johnston et al., 2015). The likelihood that auditors will impose sanctions indicates their *perceived vulnerability* to this focal threat; managers expressed varying perceptions of vulnerability:

> In general, it is difficult to catch us. (RESA)
>
> I find the risk of getting caught is too high. (RESL)

Managers who anticipate major implications of such sanctions perceived the threat as *severe*:

> These [sanctions] were major setbacks.[…] My wife got sick because of it [the sanctions]. (RESP)

In line with PMT, we observed that when managers perceived their own vulnerability to a threat that they anticipate will have severe consequences for them, they experienced some sense of fear (e.g., Boss et al., 2015; Rogers, 1983):

> [Misrepresenting work] is not allowed and there are audits, so you can get caught, so out of fear [we represent work correctly]. (RESL)
>
> To be sitting here scared out of your wits when the inspection comes in. (RESN1)

Few managers explicitly acknowledged that work misrepresentation provided them with advantages, in the form of illegal gains. In PMT terms, this benefit would represent *maladaptive rewards* of misrepresenting work:

> For us, that was our present. You earned €1000 officially and you had another €1000 illegally on top of that; and we went out for beers at night, making fun, we could go on a beautiful trip and none of it was known. And we paid almost no taxes. (RESD)

Thus, illegal monetary gains may drive at least some managers to continue their misrepresentation practices.

5.1.1.2 Appraisal of the coping behaviour 'limiting or stopping misrepresentation'

With its threat of sanctions, the government aimed to encourage managers to limit or stop their misrepresentation practices. The underlying suggestion is that adopting this focal coping behaviour would mitigate the threat of being sanctioned. However, some managers claimed uncertainty about this outcome, such that they questioned the *response efficacy* of the focal coping behaviour. As the following quote illustrates, some managers remained convinced that even if they did not misrepresent work, auditors might still believe the work was being misrepresented and impose sanctions:

> I did not adjust [increase] my prices in 2013. Why? Because, I was afraid of the reaction of the people [customers]. [When the auditor came] I have been taxed on the higher price I should have charged, but I did not charge my customers that price.[...] The fine I received for that was not too bad, but it is all the rest it brings along. I had to pay the accountant, VAT, social taxes [on the additional turnover they claimed I had made]. (RESG1)

> They catch you in a cowardly way; they need to have something.[…] The lawyer said, 'You never win against the National Social Security Office; it's better to pay'. At that time, they hadn't found any undeclared work. (RESH)

Managers' perceptions of the difficulty of halting their misrepresentation also varied. Some indicated it would be easy, but others claimed stopping misrepresentation was not always possible. Their perceived *self-efficacy* with respect to adopting the focal coping behaviour thus differed too:

> It is not difficult to do everything according to the rules. That is the easiest way, really, for me as well, for everybody, the easiest way. (RESA)

> They [employees] have to have breaks [by law], but that is impossible, of course. If they are having a break of one hour, but the customers arrive earlier, […] they [employees] have to start working. (RESH)

An overwhelming majority of interviewed managers perceived very high *response costs* of the focal coping behaviour. To justify this assertion, they referred to the high tax burden on labour income in Belgium. If managers were to declare more working hours, they would confront significant increases in payroll taxes, social security, and insurance premiums, such that their actual income would decrease significantly:

> If you pay them €10 under the table, [if you want to pay this officially] the cost for me gets multiplied by three. (RESC)

5.1.2 Contextual factors influencing the decision to adopt (or not) the focal coping behaviour

In addition to revealing the PMT core constructs related to the focal threat and coping behaviour appraisals, the interview narratives indicated that managers take other factors into account in their decision-making. We refer to these as 'contextual' factors because in PMT, a single threat appraisal and single coping appraisal are recognized to determine intentions to adopt that coping behaviour. As we illustrate in this section though, the restaurant managers actually appraised *multiple* threats and *multiple* coping behaviours when deciding whether to stop or limit work misrepresentation. In this paper, we refer to the misrepresentation sanctions as the *focal* threat and limiting or stopping misrepresentation as the *focal* coping behaviour (reflecting our primary objective of identifying the determinants of such behaviour) and consider the others as contextual factors. We chose misrepresentation sanctions as the focal threat, but arguably, another threat could have been chosen to be the focal threat. In what follows, we present the findings from the interviews related to how managers appraise the legitimacy of the focal coping behaviour, related threats, and related coping behaviours when deciding to limit or stop misrepresentation.

5.1.2.1 Legitimacy considerations

In the interviews, managers assessed the *legitimacy* of the coping behaviours expected of them, and this legitimacy assessment represented a key element influencing their intention to adopt the focal coping behaviour. According to Suchman (1995, p. 574), a behaviour appears legitimate if it is "*desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions.*" For example, RESG1 explained not adopting the focal coping behaviour by citing a belief that it would be "not fair" to employees. In contrast, RESN1 planned to stop misrepresenting work, reflecting the desire to be "no cowboys any longer … we want to be a righteous company." Although legitimacy considerations related to the focal coping behaviour do not appear in PMT, they affect managers' decisions.

5.1.2.2 Alternative coping behaviours

Most IS-PMT studies investigate appraisals of the focal coping behaviour exclusively (B1 in Figure 3), but our interviews suggest that may be insufficient, because managers clearly consider other coping behaviours (e.g., B2 and B3 in Figure 3) to mitigate the focal threat (T1). These coping behaviours can be considered as alternative coping behaviours.

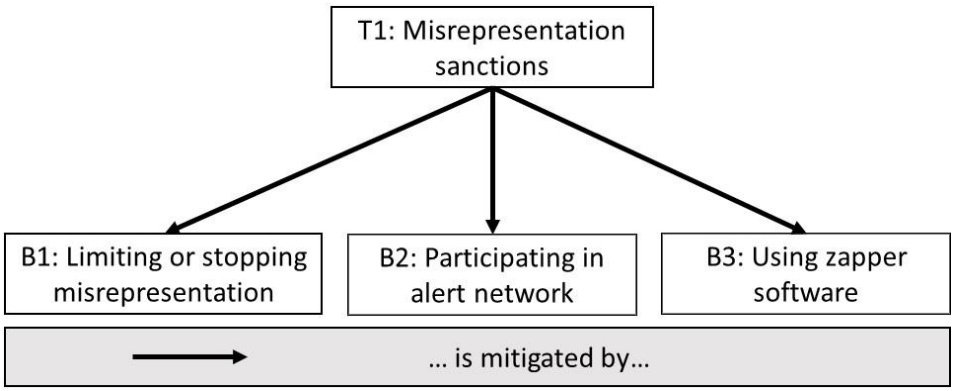

Figure 3: Alternative coping behaviours

A first alternative coping behaviour by managers involved an alert network: If managers noticed auditors in the neighbourhood, they would text warnings to other managers:

> We receive a message for inspections […]. They broadcast it automatically; it's a network. Just to warn each other. (RESD)

The use of this network mitigates the focal threat T1. Managers' intentions to limit or stop their work misrepresentation seemed to decrease when they had the option to participate in an alert network (B2, Figure 3). Using zapper software, another alternative coping behaviour mentioned by the interviewees (B3, Figure 3), enables managers to hide sales, limit traces, and mitigate the threat of misrepresentation sanctions too (T1).

In line with PMT, these alternative coping behaviours also induce their own appraisals of response efficacy, self-efficacy, and response costs. For example, managers' self-efficacy for participating in the alert network was quite high; they could easily send and receive text messages. Its response efficacy also appeared high, because it reduced the likelihood that labour auditors would catch employees working unregistered hours. Finally, the response cost of the text messages was low.

In some cases, the appraisals appeared closely intertwined across the different parties. The alert network only worked because different managers perceived the same threat and agreed to deal with it together:

> There's a lot more talking now, and people are less hesitant. Why? Because we've all been targeted, and we've all been caught. (RESD)

Thus, in intertwined appraisal processes, managers appraise the threat and the coping behaviour together (i.e., in consultation), and they also generate an alternative coping behaviour together. The appraisal processes (rounded rectangles in Figure 4) clearly overlap.

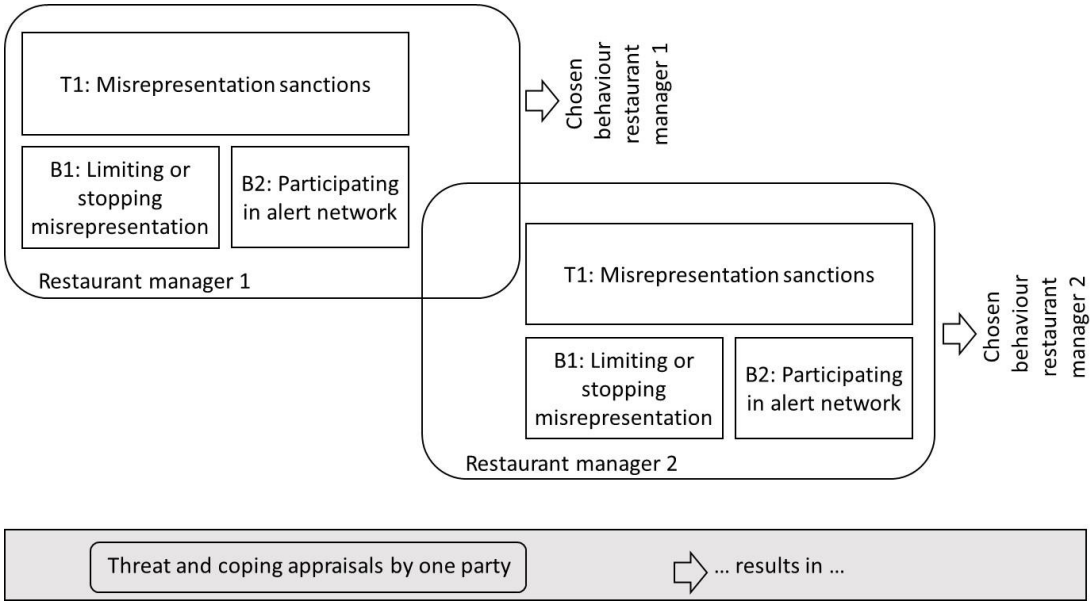

Figure 4: Intertwined appraisal processes of different parties

In other cases though, various stakeholders would unilaterally choose their behaviour, on the basis of their own threat and coping appraisals (Figure 5), and those choices could affect managers' decision-making in turn. For example, if cash register vendors install illegal zapper software, managers can hide sales more easily. When a big cash register vendor in Belgium got caught installing the software though, others refused to keep taking that risk, such that for managers, the self-efficacy of using zapper software decreased. Figure 5 is a simplified representation of these appraisal processes (rounded rectangles) by managers and cash register vendors. Both parties confront threats from the government, such that T1 manifests as a sanction for work misrepresentation by the restaurant manager and T*i* indicates a sanction for installing zapper software by the cash register vendor. If some cash register vendors decide to limit or stop installing zapper software, it affects the restaurant manager's appraisal of B3 (using zapper software). The behaviour of the cash register vendors thus influences the manager's coping appraisal, even though their appraisals are not intertwined, as shown by the nonoverlapping rounded rectangles in Figure 5. In this process, the government seemingly controls restaurant managers' behaviour by creating a threat to a third party (cash register vendors).

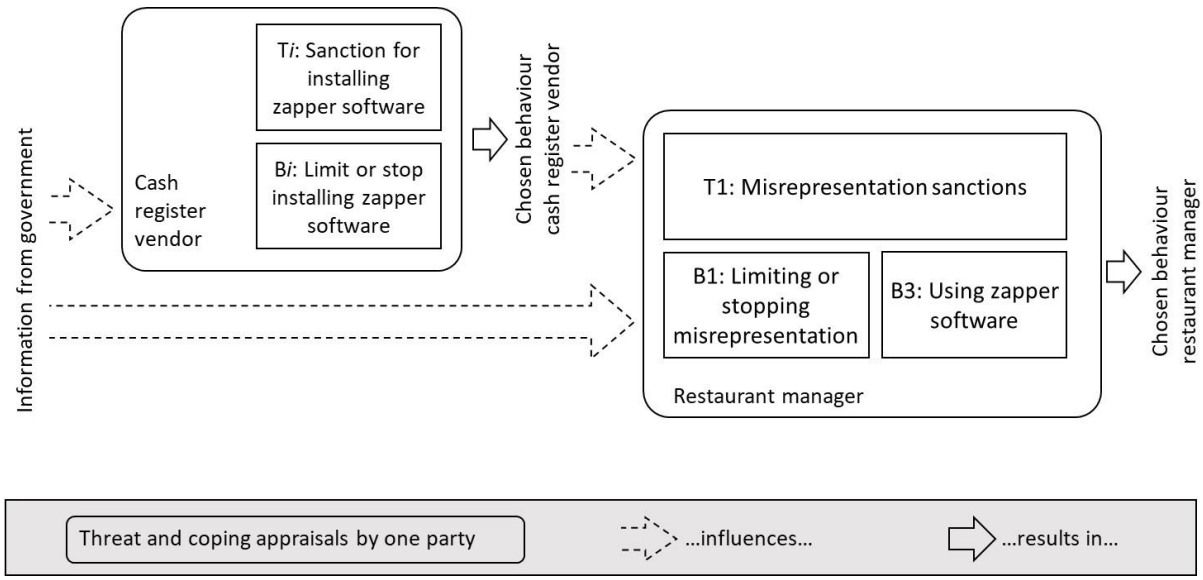

Figure 5: Related but not intertwined threat and coping appraisals by different parties

These two versions of appraisal processes suggest that, in practice, stakeholders can (try to) influence others' decisions. Stakeholders might (1) come up with a *new* alternative coping behaviour or threat that another party now must take into account or (2) influence each other's appraisals of *existing* threats and coping behaviours. Overall, the threat and coping appraisals of the different parties are highly related, and sometimes even intertwined.

5.1.2.3 Related threats

Managers do not only appraise the focal threat. In the interviews, managers also mentioned *related threat appraisals* they undertook while reflecting on whether to adopt the focal coping behaviour. Specifically, the interviewed managers account for what we call 'competing threats' and 'complementary threats' in their decision-making process involving the adoption of the focal coping behaviour.

Competing threats --- The interview evidence demonstrates that managers feel forced to pay employees under the table, because doing otherwise would create a risk of being unable to find employees. The focal coping behaviour of limiting or stopping misrepresentation (B1 in Figure 6) may mitigate the misrepresentation sanctions threat (T1 in Figure 6), but it also could magnify the threat of finding no employees (T2 in Figure 6), because employees prefer to be paid under the table. The latter T2 threat therefore functions as a competing threat.

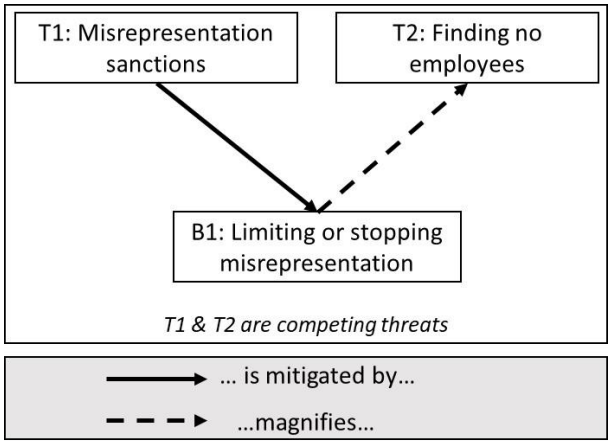

Figure 6: Competing threats

Such insights suggest that we cannot comprehend the managers' decisions if we ignore the potential that adopting the focal coping behaviour incurs a competing threat. In our research setting, many managers indicated they feared this competing threat more than the focal threat, such that it had significant influences on their decision-making process and the outcomes. Both managers and employees agreed that employees would not remain if they were forced to represent all their work 100% correctly:

> The employees tell you, if you declare each hour that we work, we will leave. (RESJ)
>
> I wonder if it [not paying under the table] won't kill the hospitality sector, in that they [managers] won't find anyone [employees] anymore. (EMPA)

Because the focal coping behaviour mitigates the focal threat (misrepresentation sanctions) but magnifies the competing threat (finding no employees), managers feel torn:

> You are torn because of your personnel. They want that [dirty money]. (RESF)

The appraisal of the competing threat goes beyond its vulnerability (chance of finding no employees) and severity (drop in revenue if customers are unhappy with bad service or because they need to limit the opening hours). In line with PMT, the appraisal of competing threats also encompasses maladaptive rewards. If managers stop misrepresenting sales, (1) they risk not finding employees, because they cannot pay employees under the table anymore, but on the positive side (2) their official revenues increase, which may give managers greater access to bank loans (and a means to make bigger investments):

> I do not have any problems with that [working more legally], because of my situation, I cannot repay 3 million euro with dirty money. (RESC)
>
> We invested more, so naturally, we need more [clean] money. (RESM)

One can regard the competing threat's maladaptive rewards (higher loans) as *additional benefits* of the focal coping behaviour (limiting or stopping misrepresentation). When discussing the coping behaviour 'limiting or stopping misrepresentation', RESL mentioned:

> So you can get caught, so out of fear [we represent work correctly] and also because we are investing. (RESL)

As this quote illustrates, the appraisal of the coping behaviour 'limiting or stopping misrepresentation' includes consideration of how it might mitigate the threat of sanctions *and* increase the possibility of obtaining higher loans.

Complementary threats --- Most managers indicate that limiting or stopping misrepresentation, by entering all orders in the cash register, would mitigate threats other than the focal threat of misrepresentation sanctions. We refer to these other threats as complementary threats (Figure 7).

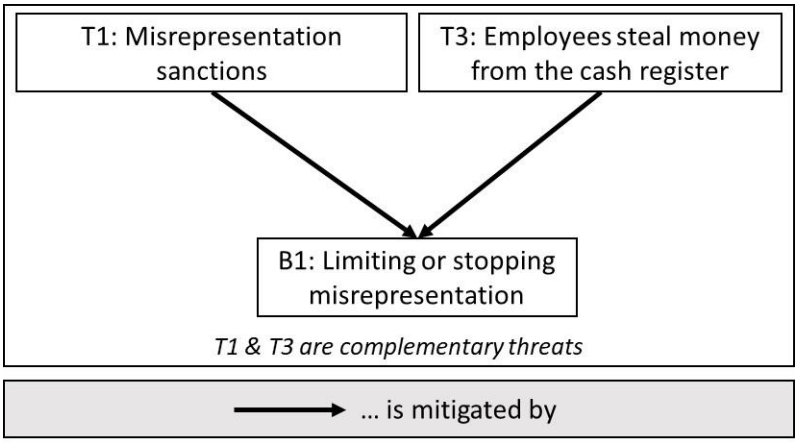

Figure 7: Complementary threats

For several restaurants, entering orders in the register is critical to their operational process, because it is how they generate order tickets for the kitchen and bar. Entering orders in the register mitigates the risk of customer dissatisfaction if they have to wait too long or receive the wrong dish. It also reduces the risk of forgetting to charge for some part of an order:

> Because I am afraid, if you don't do it that way [put it immediately in the cash register], you will just forget it. And if you don't put it on the bill, you just gave it away for free. (RESL)

Restaurants also confront threats of theft by employees (T3 in Figure 7). Integrating the cash register into the process prevents employees from omitting orders from the register and keeping the cash. Managers can verify that all cash is in the register:

> It is also a kind of verification system. If they want to cheat, the guy in the bar has to be in, and the cook in the kitchen has to be in, you understand? But they are so extremely stupid that they for instance only take away the ticket in the bar and not the ticket in the kitchen. (RESC)

The manager can easily check that the money in the cash register lines up with all tickets paid in cash. In this sense, the focal coping behaviour gives the manager a way to control employees. According to one of the civil servants, this is an important characteristic of cash registers:

> If they don't require their staff to register orders in the cash register - and that's the additional benefit we have there - then you lose your internal control over your business as well. The moment you allow waiters not to register orders, you're screwed as a business owner.[…] It would be very foolish not to require the employees to register everything. Very foolish, absolutely, absolutely. (CS2)

Therefore, the focal coping behaviour enables managers to address multiple threats simultaneously (e.g., T1 and T3, Figure 7).

5.2 Impact of RCR introduction

The government introduced the RCR regulation with the intention to enhance adoption of the focal coping behaviour (limiting or stopping misrepresentation):

> The purpose of the RCR is to tackle VAT fraud […] connected to this, the RCR is also meant to combat undeclared work in the sector […] the RCR is not a goal in itself, but rather a means to tackle a number of issues. (CS1)

> The intended goal is really to set the bar equally for everyone, to eliminate fraud […] that also has the effect of eliminating unfair competition […] [in the past] you could manipulate the numbers in your cash register. So the only thing you [the government] can do is make that more difficult, if not impossible, because that is essentially the goal.[…] In the past, especially establishments that used it as a system to manage the kitchen and the bar - it was all entered -

but at the end of the day, a large part of it was taken out again to create undeclared revenues. This is now becoming impossible […] it's entered, and we demand that the correction be made visible (CS2)

We analyse the impact of the regulation on the focal threat and coping appraisals in the next section, before considering its impacts on the contextual factors.

5.2.1 Impact of the RCR on the focal threat and coping appraisals

Two observations emerge from our analysis of the impact of the RCR on the focal threat and coping appraisals. First, managers believed that, following the introduction of the RCR, auditors would be more likely to detect work misrepresentation. Thus, they considered their vulnerability to the focal threat T1 (misrepresentation sanctions) as greater than it had been before the RCR introduction. Second, the government's efforts to compensate, in some way, for the consequences of introducing the RCR, which essentially forced managers to limit or stop misrepresenting work, influenced managers' appraisals of the focal coping behaviour B1. In detail, following some measures like lower employer taxes on overtime pay, managers perceived the response costs of adopting the focal coping behaviour decreased. Other measures, like allowing more overtime, resulted in increased perceptions of self-efficacy.

Although rarely investigated in prior research, PMT recognizes the impact of prior experiences as a source of information on cognitive mediating processes. Our interviewees offered insights into such impacts of their prior experiences. The managers understood that suddenly starting to represent work completely correctly at the moment of the RCR implementation would produce a jump in their official turnover that might trigger a tax audit. Therefore, some strategically factored the future implementation of the RCR into their current decision-making and gradually increased their official revenues in the year(s) prior to the implementation:

Over the last three years, the amount of illegal work has gone down, down, down. (RESM)

In contrast, many managers had not limited or stopped misrepresentation prior to the RCR implementation. Instead, they relied on other coping behaviours to mitigate T1 (e.g., participating in the alert network). These managers did not plan to adopt B1 immediately after the implementation either, because they did not want to display a jump in their official turnover. For example, RESE planned to

change the way employees worked during quiet times in the restaurant. During busy times, waiters would take orders using the cash register-connected app on a tablet; during quiet times, they would take orders on paper and carry them to the kitchen or bar:

> The waitresses walk around with the tablet, with Bluetooth […] if we now [with the RCR implementation] start walking around with pen and paper, you know what is happening. (RESE)

The latter orders would not be entered in RCRs, so the jump in official turnover would be limited. Thus, the choice to adopt the focal coping behaviour is contingent on prior coping behaviours adopted by the decision-makers.

5.2.2 Additional impact of RCRs

The RCR already had or would be having impacts on related threats and related coping behaviours too. For example, as vulnerability to misrepresentation sanctions (T1) increased for all managers following the RCR introduction, managers anticipated that other managers would no longer pay employees under the table, so employees would be forced to change their mindset. This prediction decreased their sensed vulnerability to the competing threat T2:

> Where will they go? It will be the same everywhere. (RESH)

Many managers were convinced that it would be harder for employees to find a restaurant that would pay them under the table. This consequence, which does not become visible when considering only the focal threat and focal coping behaviour, emerged as an extremely significant element in managers' decision-making process. Several managers reported discussions they had with employees, in which they tried to convince them that working legally would be beneficial for them. One of RESE's employees delivered food for another restaurant, which paid him under the table, prompting RESE to warn the employee about other threats (beyond getting a fine) that this behaviour could evoke:

> With a car! You can bump against a tree. I say, 'man, you are crazy?! If you bump against a tree, you are paralysed and you are not insured'. (RESE)

For RESB, the need was clear:

> You have to educate your employees, change their mentality […] of paying under the table. It is all about how you talk about it with your employees.

Following the RCR announcement, managers thus influenced employees' appraisals in an attempt to help them appreciate the benefits of working legally.

The RCR regulation affected appraisals of some alternative coping behaviours too. As noted, prior to the RCR introduction, several cash register vendors provided zappers to facilitate undeclared sales, but the RCR regulation stipulated that these vendors would be fined and lose their license to sell RCRs if caught doing so. Therefore, vendors no longer installed this functionality:

> *Interviewer:* Are there still restaurant owners that ask 'can you install that?'
>
> *Respondent:* Of course, yes, if I want to, I take 20,000 euro home tomorrow, if I visit four restaurants or so....
>
> *Interviewer:* How do you react when they ask you to do that?
>
> *Respondent:* No, no, no. No way. (CRV1)
>
> I say no, you can buy wherever you want, but I will not do that. (CRV2)

Because buying RCRs with zapper software is almost impossible, the self-efficacy of this alternative coping behaviour B3 (using zapper software) decreased. The increased severity of the threat appraisals by RCR vendors in relation to T*i* (sanctions for installing zapper software; Figure 5) affected managers' coping appraisals.

Ultimately then, in addition to influencing focal threat and coping appraisals, the RCR regulation affected related threat and coping appraisals and thereby influenced managers' adoption of the focal coping behaviour. To understand the impact of the RCR introduction on managers' decision-making process, we must consider its impacts on other, contextual elements.

6. Discussion

Due to the presence of contextual factors, the focal threat and coping appraisals, as discussed in PMT, may not accurately explain actors' intentions to adopt the focal coping behaviour. Conflicting findings in prior IS-PMT studies may reflect this influence; when studies concentrate on one focal threat and one focal coping behaviour, they skip over the potentially substantial effects of related threat and coping appraisals. In suggesting the presence of boundary conditions, our findings reveal a need to contextualize PMT and establish a "*more context sensitive*" framework (Whetten, 2009, p. 36). In this section, we

propose the RTCAF (Related Threat and Coping Appraisals Framework), starting with a high-level view, then moving to a more detailed discussion of its different aspects. In our contextualization efforts, we follow Hong et al.'s (2014) guidelines for context-specific theorizing (Sections 6.2-6.7). The identified contextual factors reveal boundary conditions of PMT, as well as pertinent adjustments for applying PMT to IS research (Busse et al., 2017; Hong et al., 2014). We outline practical implications in Section 6.8 and then discuss limitations and further research opportunities in Section 6.9.

6.1 The RTCAF

Figure 8 contains the Related Threat and Coping Appraisals Framework (RTCAF). This framework results from our abductive research process, in which we iterated back and forth between the empirical evidence and our theoretical knowledge. The RTCAF recognizes that the intent to adopt a focal coping behaviour depends on the focal threat and coping appraisals, as advocated in PMT, but also on the perceived legitimacy of that coping behaviour (Section 6.2), appraisals of alternative coping behaviours (Section 6.3), appraisals of competing threats (Section 6.4), and the presence of additional benefits (Section 6.5) and complementary threats (Section 6.6). For simplicity, Figure 8 does not make the elements of the related threat and coping appraisals explicit, but they are part of the managers' appraisals. In Section 6.7, we also discuss the information sources on the left side of Figure 8. Table 5 summarizes the findings and illustrates the RTCAF in our research context.

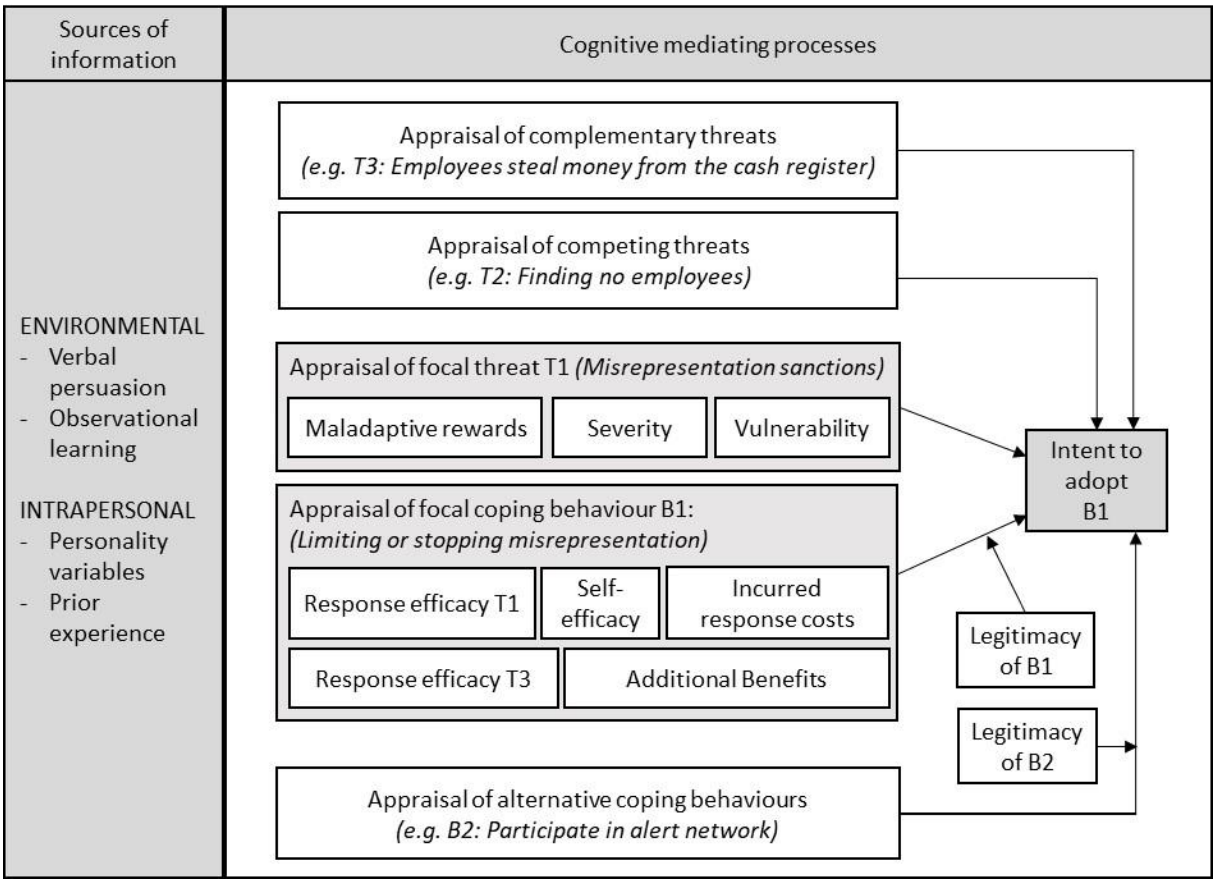

Figure 8: RTCAF - Grey rectangles are part of PMT; italics indicate examples from our research setting.

Focal Threat Misrepresentation sanctions	is mitigated by	Focal coping behaviour	Limiting or stopping misrepresentation
		Alternative coping behaviours	Managers can use zapper software to avoid misrepresentation sanctions. Such software helps delete sales from the cash register, renumbers receipts, and produces confirming financial reports, so auditors cannot find inconsistencies.
			Managers can participate in an alert network to avoid misrepresentation sanctions, in which managers of different restaurants text each other if they notice labour auditors in the neighbourhood. Managers then register all employees' work correctly in the computer system at that moment and move illegal labour to other time slots (and might increase illegal labour at other moments).
Focal Coping Behaviour	mitigates	Focal threat	Misrepresentation sanctions
	magnifies	Competing threats	Employees prefer to be paid under the table. If managers limit or stop misrepresenting work (i.e., do not pay sufficiently under the table), they run the risk that employees will not want to work in their restaurant.

	appraisal involves	Legitimacy	Some managers do (not) regard limiting or stopping misrepresentation as desirable, proper, or appropriate, according to some socially constructed system of norms, values, beliefs, and definitions.
	comes with	Additional benefits	If managers limit or stop misrepresenting work, they can get higher bank loans (and make bigger investments), because their official revenues are higher.
	also mitigates	Complementary threats	If managers limit or stop misrepresenting work, the data in the system limit the risk of poor service (delays, wrong dishes).
			If managers limit or stop misrepresenting work, the data in the system limit the risk they will forget to charge for part of an order.
			If managers limit or stop misrepresenting work, it reduces the threat that employees will steal money.

Table 5: Illustration of RTCAF cognitive mediating processes

6.2 Legitimacy

Decision-makers are unlikely to adopt the focal coping behaviour if they perceive that it is not in line with what they regard as legitimate. Perceived legitimacy constitutes a motivational force (Tyler, 2002), which Son (2011) identifies as an even more significant antecedent of IS security policy compliance than sanction certainty and severity. Similarly, "role values" (a construct that overlaps conceptually with legitimacy, referring to perceptions that policy compliance is appropriate) exert strong impacts on intentions to comply (Moody et al., 2018). Other protection motivation studies in IS highlight concepts related to legitimacy, such as perceived organizational justice and moral obligation. For example, intentions to comply with an Internet policy depend on perceived organizational justice, which has been linked theoretically to legitimacy (Hegtvedt & Johnson, 2009; Levi et al., 2009). Moral obligation relates significantly to computer security behavioural intentions (Yoon & Kim, 2013) and faculty members' adoption of anti-plagiarism software (Lee, 2011). It also conceptually overlaps with moral legitimacy (one of three legitimacy types defined by Suchman, 1995).

Our interviews suggest that perceived legitimacy functions as a boundary condition of the relation between a coping appraisal and the intention to adopt the focal behaviour (Busse et al., 2017). If decision-makers perceive the behaviour as illegitimate, the PMT coping appraisal constructs are unlikely to explain intentions to adopt the focal coping behaviour accurately. In line with Hong et al.'s (2014)

guidelines, we suggest that quantitative studies should incorporate the legitimacy construct as a moderator, to increase the generalizability of their research models (see Figure 9).

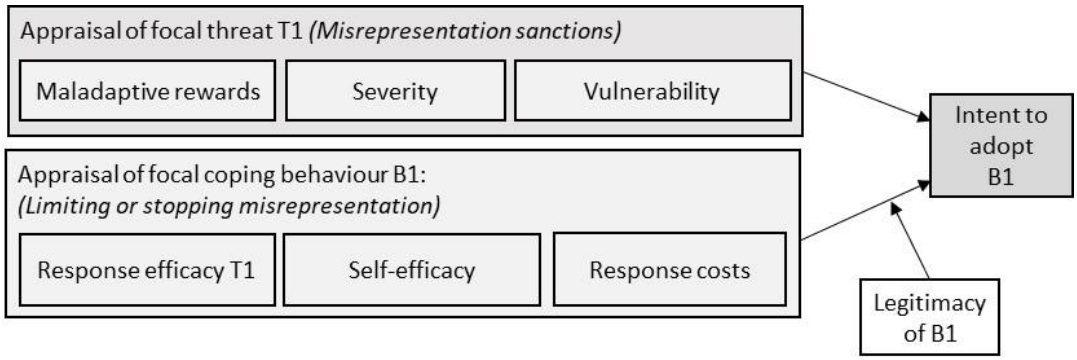

Figure 9: Legitimacy as a moderator of PMT components in cognitive mediating processes

6.3 Appraising alternative coping behaviours

Restaurant managers appraise several coping behaviours when deciding whether to limit or stop misrepresenting work. To capture this insight, we define a generic concept of *alternative coping behaviours*: When considering focal threat T1 and focal coping behaviour B1, behaviour B2 is an alternative coping behaviour if B2 also mitigates T1. Figure 10 shows the misrepresentation sanction threat can be mitigated not just by limiting or stopping misrepresentation but also by participating in an alert network. The IS used in alert networks (i.e., cell phones) afford managers the capability to predict when auditors will show up on their premises, which allows them to mitigate the focal threat.

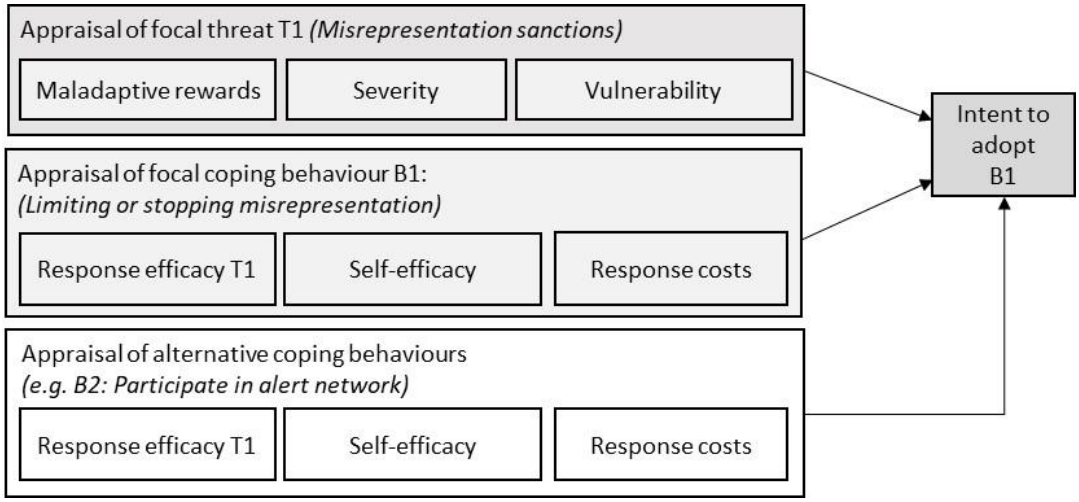

Figure 10: Alternative coping behaviour appraisal together with PMT components in cognitive mediating processes

Notably, PMT acknowledges that actors can appraise several adaptive coping behaviours (Rogers & Prentice-Dunn, 1997), and a few IS-PMT studies have noted the existence of such alternative coping behaviours, by building models with different dependent variables (Youn, 2005). Other studies implicitly recognize the existence of alternative coping behaviours by describing general coping behaviours (e.g., "protective actions"), together with several specific examples (e.g., "have a firewall," "install spam-filter software," "installed antivirus software") (Chen & Zahedi, 2016). In their application of PMT, Nehme and George (2022) implicitly explain motivations to adopt two coping behaviours to deal with threats created by smart home devices. We note Aurigemma and Mattson (2019, p. 1734) call for studies to focus on specific coping behaviours (e.g., "*Use caution when visiting sites with expired certificates*," "*Do not access the web by selecting links in emails*") rather than general ones (e.g., "*I intend to comply with the ISP*"). Notably, at a more specific level, the presence of alternative coping behaviours is more likely, so recognizing alternative coping behaviours appears particularly relevant for PMT studies. Thus, some PMT studies recognize the *existence* of alternative coping behaviours, yet like the theory itself, these studies do not explicitly identify how the appraisal of one coping behaviour can influence the adoption of another. In a notable exception, Herath et al. (2014) indicate that email screening self-efficacy is a significant antecedent of users' intentions to adopt another coping behaviour, namely, email authentication services.

For a given threat appraisal and focal coping appraisal, a decision-maker who perceives no other coping behaviours might adopt the focal one, but another decision-maker who uncovers alternative coping behaviours might not adopt the focal coping behaviour. When decision-makers perceive appealing alternative coping behaviours, the accuracy of PMT will be low, pointing to a boundary condition. To ensure that the range of our theoretical framework is not limited to settings in which no significant alternative coping behaviours exist (Busse et al., 2017), the RTCAF explicitly recognizes that alternative coping appraisals can influence intentions to adopt focal coping behaviours, which is in line with Hong et al.'s (2014) guidelines for context-specific theorizing. We accordingly call for research to incorporate this contextual factor as an antecedent of the dependent variable in quantitative studies.

6.4 Appraising competing threats

The interviewed managers were struggling with the concern that, even if the focal coping behaviour (B1, limiting or stopping misrepresentation) mitigated the focal threat (T1, misrepresentation sanctions), it would magnify another threat (T2, finding no employees) (Figure 11). Therefore, we define a generic concept of *competing threats*: When considering focal threat T1 and focal coping behaviour B1, threat T2 is a competing threat if T1 is mitigated by B1, but B1 magnifies T2.

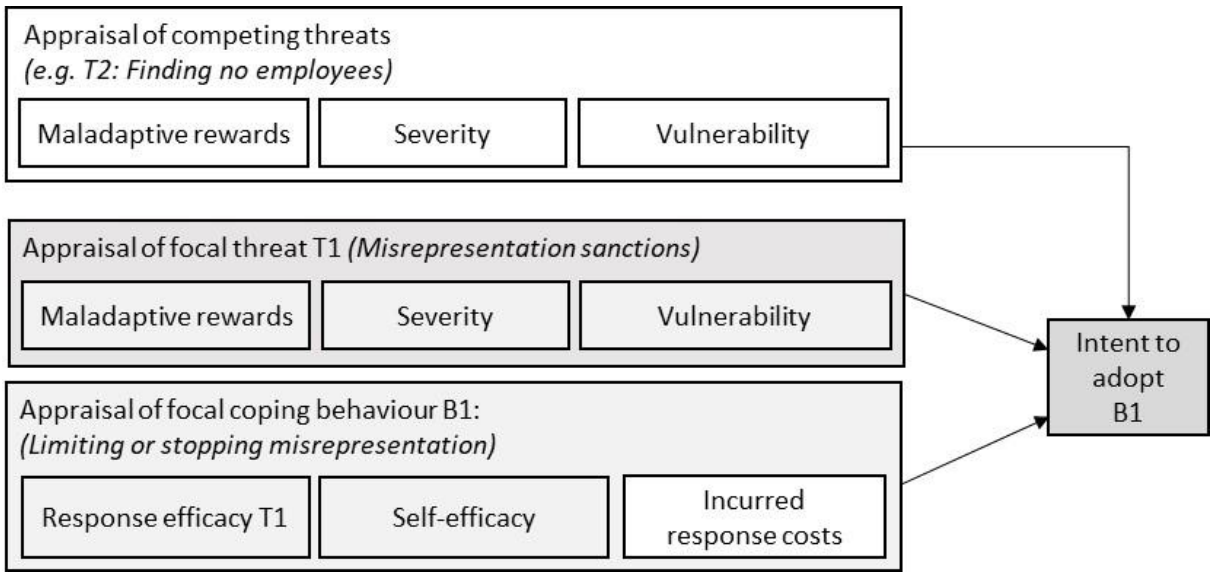

Figure 11: Competing threats together with PMT components in cognitive mediating processes; response costs are refined to 'incurred response costs'

By actualizing IS' affordances to register data, managers magnify the threat of not finding employees. If the IS offered the capability to erase data, the competing threat could be mitigated. Yet, restaurants that did not misrepresent sales (for instance because they did not have zapper software) had a competitive disadvantage, which the government sought to remedy by introducing the RCR, to level the playing field. As all restaurants are now required to use RCRs, which do not afford managers the capability to erase revenues from their cash register, restaurants should not get illegal money anymore to pay employees under the table so that the competing threat should disappear. By eliminating an affordance provided by previous IS, the competing threat was (supposed to) disappear.

Recognizing such competing threats is crucial for understanding managers' decision-making. Arguably, they are implicitly present in PMT, in that they might be considered a type of response cost. Rogers and Prentice-Dunn (1997, p. 116), recognizing that the response costs construct is muddled, suggest that

"*one of the major frontiers for future research will be to find different facets of PMT components.*" Similarly, Lowry et al. (2023, p. 1123) conclude that "*Response costs, as currently operationalized, are ineffective maladaptive predictors across the literature and thus need to be omitted, reconceptualized, or better measured in the ISM context.*" In line with Busse et al.'s (2017, p. 593) discussion, these concerns imply the need for a boundary condition–related refinement of a construct that is "*too unspecific to be employed in any context, precisely because it can be infused with various meanings.*" In further support of this interpretation, we note that response costs have been measured very differently across studies. Hanus and Wu (2016) use five items, all of which refer to financial costs, but Lee (2011) relies on items pertaining to overhead, time, effort, and behaviours that might lead to distrustful relationships. In line with Hong et al.'s (2014) guidelines, we therefore propose decomposing PMT response costs into two constructs: competing threats and incurred response costs. For both components, the size of the cost is hard to determine. However, whereas the chance of occurrence is 100% for incurred response costs, the occurrence of competing threats is uncertain (and appraised by perceived vulnerability). Notably, this conceptualization aligns with the Oxford Dictionary definition of threat as the *possibility* of trouble, danger, or ruin.

The Appendix illustrates the potential for competing threats to arise in diverse IS settings. Yet previous IS research has not explicitly investigated this concept. Gao et al. (2015) de facto recognize two threats that compete (privacy vs. health threats) as antecedents of intentions to adopt wearable technology. Relatedly, while mobile health devices can mitigate health threats, Fox and Connolly (2018) find that beliefs about risks associated with disclosing health information have a negative impact (via privacy concerns) on intentions to adopt mobile health devices. Lee (2011) concentrated on plagiarism threats to explain anti-plagiarism software adoption, but the study respondents raised a competing threat, namely, their concerns that commercial anti-plagiarism software vendors would misuse their submitted materials

Studies that do not control for competing threats may fail to reveal the potentially significant relations between a focal threat appraisal and intentions to adopt a focal coping behaviour. This also might explain why threat vulnerability and severity do not appear significantly related to coping behaviour adoption

in several studies (Crossler et al., 2014; Tsai et al., 2016; Zhang & McDowell, 2009). If decision-makers are considering significant competing threats, PMT's accuracy will be low because constructs representing competing threat appraisals are not included in the study. Our findings highlight the importance of recognizing how competing threat appraisals can alter intentions to adopt a focal coping behaviour.

6.5 Additional benefits

Danger mitigation is not the only reason to engage in a focal behaviour. Decision-makers consider *additional benefits*, which we define as benefits derived from the coping behaviour, beyond threat mitigation. In health domains, where PMT originated, additional benefits might not always be relevant, but in IS domains, information systems often afford more capabilities than mere protection against threats. Additional benefits have been studied sporadically in relation to protection motivations in the IS field, such as IT security compliance (Chen et al., 2012; Pahnila et al., 2007) or ERP policy compliance (Liang et al., 2013). Furthermore, in what is, to the best of our knowledge, the only qualitative IS-PMT study thus far, Posey et al. (2014) signal the need to include additional benefits to explain coping behaviours, by suggesting "*other motivators*" beyond the six PMT constructs. Some of these motivators pertain to additional benefits (e.g., "*A formal financial incentive or time off incentive for successfully passing random security audits*"; Posey et al., 2014, p. 562).

Coping theory suggests that primary appraisals involve evaluations of the potential consequences of an event (e.g., RCR introduction) and also recognizes that events can have negative or positive consequences (Beaudry & Pinsonneault, 2005; Lazarus & Folkman, 1984). Similarly, in PMT, maladaptive rewards associated with risky behaviour strongly predict protection motivations (Lowry et al., 2023). We argue that additional benefits associated with coping behaviours - rather than only maladaptive rewards associated with risky behaviours - should be recognized. If the research goal is to explain why actors adopt a focal coping behaviour, the study must assess whether those decision-makers perceive additional benefits beyond threat mitigation that drive their adoption. If decision-makers perceive significant additional benefits, the accuracy of PMT will be low, suggesting a boundary condition.

Additional benefits (e.g., more bank loans) of the coping behaviour (in casu: limiting or stopping misrepresentation) can manifest as maladaptive rewards of a competing threat appraisal (e.g., not finding employees without misrepresenting work). In our research context, the focal coping behaviour also magnifies a competing threat. Therefore, additional benefits associated with the focal coping behaviour may appear (in PMT terminology) like maladaptive rewards of competing threats. In other real-world contexts, *even without competing threats* (and thus no maladaptive rewards of competing threats), additional benefits (beyond threat mitigation) still could be associated with the focal coping behaviour. These additional benefits then would be appraised within the coping appraisal (Figure 12).

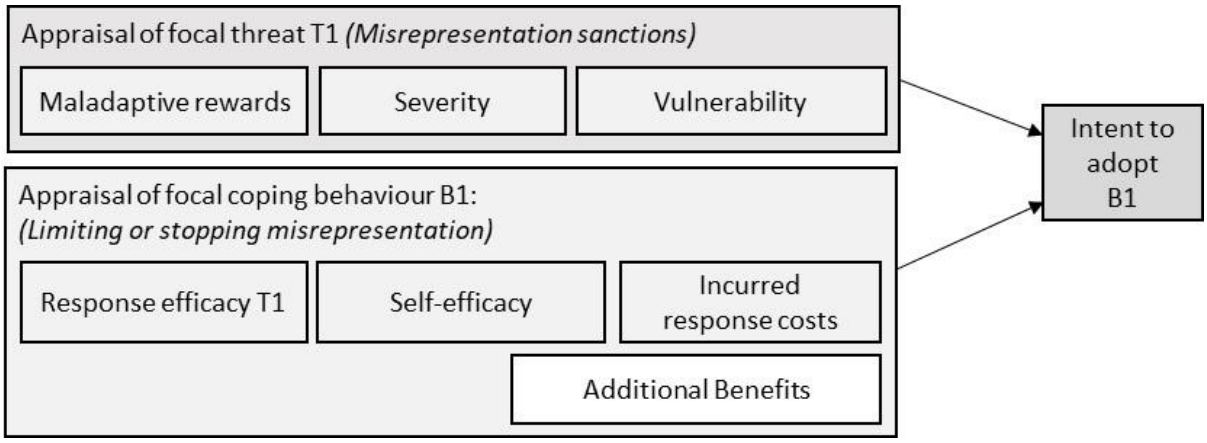

Figure 12: Additional benefits as part of the coping appraisal

For completeness, we reiterate that we removed competing threats from the PMT response costs construct in Section 6.4. Reflecting prior observations that the response costs construct is muddled, we also note that Posey et al. (2015, p. 197) state that "*individuals' formation of response costs is a cost–benefit analysis, wherein benefits are linked to potential rewards and costs.*" Therefore, additional benefits should be included as further antecedents of intentions to adopt a behaviour, in line with Hong et al.'s (2014) fourth guideline for developing context-specific models.

6.6 Appraising complementary threats

Managers recognize that a single coping behaviour (limiting or stopping misrepresentation) can mitigate multiple threats, such as misrepresentation sanctions (T1 in Figure 13) but also theft by employees (T3 in Figure 13). Stated differently, the risky behaviour of misrepresenting work increases multiple threats. By circumventing the rules, managers not only dilute the effectiveness of the government's control but

open doors to other risks (Dey et al., 2022). In relation to threat T3 (theft by employees), the behaviour of entering all sales in the cash register system transforms the cash register system into a true "electronic panopticon," engaged in surveillance of employees, which reduces the need for direct supervision (Sewell & Wilkinson, 1992). Much like the classic panopticon (Bentham, 1780), an employee's bad behaviour (e.g., stealing from the cash register) would be visible anytime, and employees know that they can be watched, even if they do not know when. In this situation, employees likely internalize a sense of constant monitoring, so the cash register fosters self-discipline by employees, reducing the need for continuous, active surveillance. We identify a double panoptic effect, because the data gathered by the RCR also enables surveillance of managers. A visiting auditor can visually compare the food served to tables or in preparation in the kitchen with orders in the RCR. A manager's bad behaviour (i.e., not immediately entering orders in the RCR) becomes immediately visible to the auditor. Here again, there is no need for continuous, active surveillance, because managers know they can be checked anytime, so they are motivated to engage in self-discipline.

The government has taken such double panoptic effects into account. As noted, the civil servants we interviewed believe that restaurant managers would be "very foolish" to misrepresent sales in the cash register, as it opens the door for theft by employees. The government anticipates that managers' desire to control employees (i.e., to mitigate the complementary threat) will motivate them to register sales in the system. Before the introduction of the RCR, managers could still delete orders later (e.g., with phantom-ware, which affords managers the capability to delete orders after closing, when all employees had left), but following the introduction of the RCR, this action is no longer possible. By making sure the new IS does not afford managers the capability to delete data unnoticed, the government can better control restaurants that enter data in the system, while also enabling restaurant managers to control employees through the same system.

These threats are complementary to the limiting or stopping misrepresentation coping behaviour. We thus can define a generic concept of *complementary threats*: When considering focal threat T1 and focal coping behaviour B1, threat T3 is a complementary threat if both T1 and T3 can be mitigated by B1.

Each threat evokes a different level of response efficacy though. Therefore, the response efficacy evaluation in the coping appraisal takes place separately for each complementary threat (Figure 13).

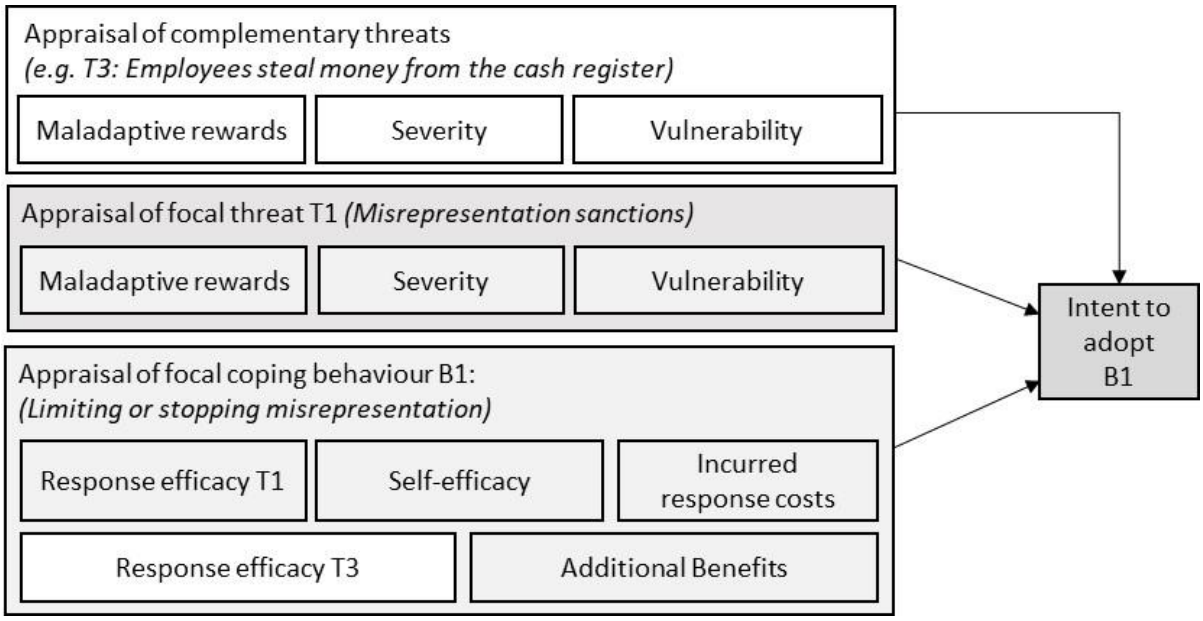

Figure 13: Complementary threats mitigated by the focal coping behaviour

Mitigating complementary threats could be a benefit of the coping behaviour, beyond the mitigation of the *focal* threat. However, we argue that complementary threats are important on their own right in the decision-making process, so we propose decomposing the benefits of the coping behaviour, beyond the mitigation of the *focal* threat, into two constructs: *additional benefits* (as defined previously) and mitigation of *complementary threats*. Following Hong et al.'s (2014) fourth guideline, we separate out complementary threats (rather than regarding them as part of the additional benefits), and we defined additional benefits as those beyond the mitigation of threats *in general* (rather than benefits beyond the mitigation of the *focal* threat).

The Appendix illustrates the potential presence of complementary threats in diverse IS settings. Previous IS research has not investigated this concept directly, though some studies de facto model complementary threats (e.g., including sanctions together with information security threats) as (indirect) antecedents of intentions to comply with security policies (Herath & Rao, 2009; Johnston et al., 2015; Pahnila et al., 2007). If decision-makers perceive significant complementary threats, the accuracy of PMT will be low because decision-makers would adopt the focal behaviour for reasons other than mitigating the focal threat, pointing to a boundary condition. Therefore, we suggest explicitly

recognizing that complementary threat appraisals can influence intentions to adopt a focal coping behaviour.

6.7 Information sources

In line with PMT, we find that different information sources affect cognitive mediating processes. Fear appeals (a type of verbal persuasion) have received substantial attention in PMT studies, and though we also observe them in our setting, we seek to shed new light on other information sources that have received less prior attention in IS-PMT literature. For example, PMT designates adopted coping behaviours as prior experiences, such that they constitute an information resource that can influence decision-making processes (Rogers, 1983). Although Rogers and Prentice-Dunn (1997, p. 114) describe prior experiences as "*perhaps the most underappreciated component*" and worry that feedback from coping activity "*remains largely unexplored*," PMT studies rarely address prior experiences. Perhaps researchers assume that prior coping behaviour merely lowers perceived vulnerability. However, our findings indicate that the reality is more complex, and previously adopted coping behaviours must be taken into account to gain a full understanding of the decision to adopt a focal coping behaviour. Depending on their prior behaviours, adopting the focal coping behaviour might appear to increase, rather than mitigate, the threat (e.g., because suddenly registering all sales would create an unexplainable jump in official revenues).

Furthermore, prior IS-PMT studies include concepts that suggest an influence of others (e.g., descriptive norms, social influence, subjective norms, normative beliefs). To some extent, these concepts can be regarded as 'sources of information' in PMT (see Figure 1). Descriptive norms reflect the decision-maker's beliefs about the extent to which peers are performing the focal behaviour. Subjective norms, social influence, and normative beliefs pertain to the decision-maker's perception of what important others think that they should do. Relative to prior IS-PMT studies, our findings thus suggest two main conclusions.

First, IS-PMT studies that investigate descriptive norms (Anderson & Agarwal, 2010; Herath & Rao, 2009), social influence (Barlette et al., 2017; Gao et al., 2015; Johnston & Warkentin, 2010; Komatsu et al., 2013; Lee, 2011; Lee & Larsen, 2009), subjective norms (Anderson & Agarwal, 2010; Chen et

al., 2020; Grimes & Marquardson, 2019; Herath & Rao, 2009; Ifinedo, 2012; Safa et al., 2015; Sun et al., 2013; Tsai et al., 2016; Yoon et al., 2012; Yoon & Kim, 2013), and normative beliefs (Pahnila et al., 2007; Siponen et al., 2014) model them as *direct* antecedents of behaviour or behavioural intentions. In most of these studies, the direct relation is significant (cf. Lee, 2011; Yoon et al., 2012; Yoon & Kim, 2013). Yet, we find (in line with PMT) that these concepts also have important *indirect* impacts on behavioural intentions. In our study, the descriptive norms appear to affect behavioural intentions indirectly through the intensification or mitigation of threats. If peers (i.e., other managers) behave in a specific way (e.g., misrepresent work), a threat (not finding employees) arises for the focal decision-maker. This threat does not stem from the behaviour of an isolated manager. It arises because a significant number of peers pay under the table. Following the introduction of RCRs, managers believed other managers would (start to) work legally, and this shift in the descriptive norm implied that their perceived vulnerability to the threat of finding no employees decreased significantly. In turn, managers felt less pressure to misrepresent work. Similarly, descriptive norms may have indirect impacts on behaviour through coping appraisals. Participating in an alert network only offers high perceived response efficacy if peers also participate. Likewise, the impacts of social influence, subjective norms, and normative beliefs on behaviours encompasses more than just direct relations. If cash register vendors opt not to install zapper software, signalling their preference that managers work legally, then managers' self-efficacy for using zapper software, as a coping behaviour, necessarily decreases. In addition to the direct impacts identified in several IS-PMT studies, we reveal how stakeholders can exert indirect impacts on PMT core constructs, which in turn indicates that restaurant managers' behaviour reflects, at least to some extent, the expectations of those stakeholders. By showing that, in addition to direct impacts identified in prior IS-PMT research, stakeholders can alter PMT's cognitive mediating processes, we confirm the idea that environmental information sources other than fear appeals affect the cognitive mediating processes.

Second, previous IS-PMT research tends to assign "important others" a passive or, at most, a supporting role (Johnston & Warkentin, 2010; Lai et al, 2012). Our study instead reveals that different parties can be regarded as information sources for one another but also that managers' threat and coping appraisals

might become closely intertwined, such that they actively develop new coping behaviours (and potentially new threats for others) in collaboration. By developing coping behaviour together (e.g., alert network), managers find ways to deal with threats. In PMT, the environment functions as a given source of information and possible coping behaviours are predefined. In practice though, we identify two-way interactions that can lead to new alternative coping behaviours (which are hard to account for in quantitative PMT studies). In the health domain, where PMT originated, patients could hardly be expected to come up with alternative coping behaviour themselves, but in the IS domain, the situation is clearly different.

6.8 Implications

The boundary conditions identified by this study have significant implications for IS-PMT researchers. In particular, these insights might help explain conflicting findings in prior quantitative studies that concentrate on one focal threat and one focal coping behaviour, without accounting for the potentially relevant effects of related threat and coping appraisals. As an illustration, the Appendix outlines some related threats and coping behaviours that might arise in other settings. In Figure 14, we also offer a simplified version of the RTCAF to provide a high-level illustration of how our main findings could apply in a different setting. In detail, a PMT study could investigate intentions to back up data in the cloud (Menard et al., 2014) by assessing appraisals of this coping behaviour and the threat of data loss due to a hard disk crash (grey rectangles in Figure 14). Our paper argues that prior studies have not heeded the possibility that decision-makers would simultaneously appraise related threats and coping behaviours (white rectangles in Figure 14). If they believe they can mitigate the threat of data loss due to a hard disk crash by using a more shock-proof technology, such as an SSD installed in their PC, these decision-makers would not adopt the behaviour of backing up data in the cloud. Even if they do intend to back up their data in the cloud, that intention might stem from an attempt to mitigate the data loss due to a hard disk crash threat, or it could originate from a desire to mitigate the threat of malware encrypting data on their PC. In turn, backing up data in the cloud, as a coping behaviour, might mitigate the threat of hard disk crashes, but decision-makers could worry that it also increases the threat of their data being stolen from the cloud, which likely decreases their behavioural intentions. When the threats and coping

behaviours represented in the white rectangles are salient, research that focuses exclusively on appraisals of the threat of data loss due to a hard disk crash and the coping behaviour of backing up data in the cloud (grey rectangles in Figure 14) cannot accurately explain the ultimate decision people make.

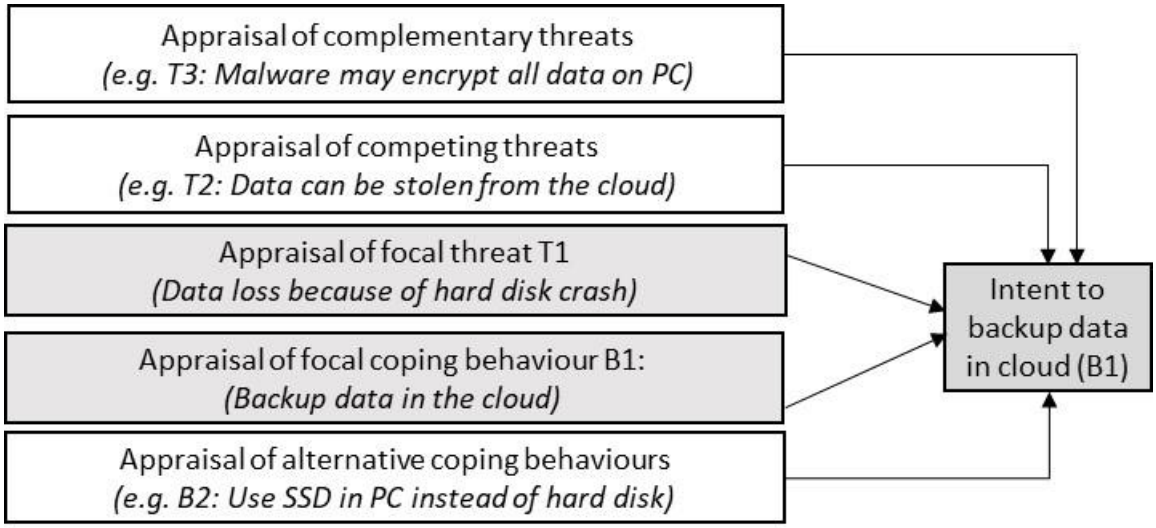

Figure 14: Appraisal of PMT focal threat and focal coping behaviour (grey rectangles) and context (white rectangles) in alternative setting

Our study also has three main implications for practitioners. In line with evidence that organizational security efforts focused on deterrence alone tend to be ineffective for preventing insider computer abuse (Burns et al., 2023), we find, in a Belgian restaurant setting, that deterrence appears insufficient for bringing about the desired coping behaviour, that is, limiting or stopping work misrepresentation. The insights embedded in the RTCAF suggest some practical implications in control-based settings, marked by controllers (e.g., corporate management, government) who want controlees to adopt specific behaviours (Kirsch, 1997).

First, the controllers (the government in our study) must consider more than the focal threat and coping behaviour if they want to encourage the focal coping behaviour. As the RTCAF indicates, to influence others' behaviour, these controllers may not only seek to influence the focal threat and coping appraisals but also reflect on how they might induce negative appraisals of alternative coping behaviours and competing threats while simultaneously encouraging positive perceptions of the additional benefits and legitimacy of the desired behaviour, as well as positive appraisals of complementary threats. Government agencies and the restaurant sector federation in Belgium appear to understand that different appraisals and perceptions influence restaurant managers' decisions. For example, the government

recognized that managers' appraisals of using zapper software, as an alternative coping behaviour, were too positive, so it decided to introduce the RCR, which made such uses nearly impossible. The sector federation also emphasized additional benefits (e.g., bank loans) to convince managers to limit or stop their work misrepresentation.

Second, managers only actualize affordances that align with their existing goals and intentions (Mesgari et al., 2023). Even before the RCR introduction, the government tried to prompt managers to actualize the registration affordances offered by IS. In line with the Deleuzian control society concept, we argue that the government could have encouraged such actualizations by adhering to a rhizome metaphor (i.e., by moving away from a top-down logic). Consistent with Leclercq-Vandelannoitte's (2013) observations in the consulting industry, restaurant customers might have been deployed as a means to impose pressure on or control restaurants. In Portugal and Malta for example, governments run a lottery based on restaurant cash register tickets, such that consumers are motivated to ask for receipts and share them with the government. This panopticon leads restaurant managers to sense that they can be permanently monitored. The Belgian government did not opt to involve restaurant consumers though; it maintained a top-down logic in issuing the misrepresentation sanction threat, which then limited the control the government could exert over the actualization of the registration affordances. Work misrepresentation could only be detected if auditors caught restaurants red-handed or found inconsistencies in the numbers, which restaurants could prevent by using zappers. The top-down approach might become more successful with RCR in place. As stated previously, the RCR acts as a true electronic panopticon. The government relies on managers' desire to control their employees as motivation to register sales, and these sales can no longer be deleted. By making sure the RCR does not afford managers the capability to delete data unnoticed, the government exerts better control over restaurant managers who still want to actualize the IS registration affordance because those affordances are in line with their goal to control restaurant employees through the same IS. Furthermore, our study suggests controllers could seek to shape controlees decision-making processes by exerting influence over environmental resources and stakeholders whose behaviours influence the focal decision-makers. In our research setting, the government sought to control managers' behaviour indirectly by targeting

other stakeholders (register vendors), such that it established 'control through networks' (Håkansson & Ford, 2002; Kirsch, 1997).

Third, the RTCAF provides insights for designing effective communication purposes. After an incident, stakeholders may develop a bad impression of the company if they learn that it had not adopted a (focal) coping behaviour. We propose that firms could leverage the RTCAF elements to alleviate the damage to their image. For example, they could explain their choice not to adopt the focal coping behaviour by pointing to alternative coping behaviours they did implement (but that turned out to be ineffective), complementary threats that they were able to mitigate through the alternative coping behaviour, or competing threats associated with the focal coping behaviour. Stakeholders might understand firms' decisions better if they get a picture of the complex web of threats and coping behaviours that they face.

6.9 Limitations and further research

As every study, our study has some limitations. Some of which can be regarded as avenues for future research. First, our study remains purposefully and firmly focused on one setting, which enables us to identify diverse related threats and coping behaviours. Additional quantitative research is needed to perform empirical tests of the relevance of related threats and coping behaviours, and the RTCAF overall, in other settings. Second, we detail decision-making processes without specifying which factors represent the strongest choice determinants. Additional research might clarify which factors drive such decisions most powerfully. For example, managers perceived the RCR introduction as a threat initially, but a longitudinal investigation could determine if this perception shifted, such that they came to see it an opportunity, as positive outcomes emerged. The emergence of new technology might seem like a threat or an opportunity, and these perceptions may evolve, so the strongest determinant (e.g. additional benefits) might shift over time too. Third, the notion of interactions with the environment are in line with PMT, but our interviewees mentioned several such interactions that have not been recognized by PMT. For example, the alert network works because multiple managers perceive the same threat and collaborate to address it, such that their appraisal processes for both the threat and the coping behaviour are intertwined. Therefore, the environment is not just a source of information (as recognized in PMT) but also a collaborative factor. We call for additional research into such shared appraisal processes.

Fourth, prior research suggests that the impact of social influence (and other PMT constructs) depends on the decision-maker's characteristics, such that social influence emerged as a significant antecedent of protection motivations among small firms' owner-CEOs but not non-owner-CEOs (Barlette et al., 2017). Our data set does not provide sufficient insights to draw conclusions about the difference between owner-managers and non-owner-managers. Fifth, new threats and coping behaviours are emerging, suggesting the need for research into how the act of generating threats and alternative coping behaviours can be integrated with the RTCAF. Sixth, sanctions represent the focal threat in our study, which suggests the potential relevance of Deterrence Theory in our context. Two of its three fundamental concepts emerged from our interviews (i.e., sanction severity and sanction certainty, which overlap conceptually with PMT constructs), whereas a third (sanction celerity) did not. It would be worthwhile to investigate if, in other contexts, celerity arises, such that it arguably should be included in the RTCAF. Seventh, PMT researchers disagree about the role of fear: Lowry et al. (2023, p. 1123) argue that "*Fear should be assumed to be and modelled as a full mediator of the threat -> PM relationship,*" but Siponen et al. (2024, p. 1145) assert that "*fear may not be a particularly relevant concept*" and "*that attitude change is not mediated by or a result of an emotional state of fear.*" According to Beaudry and Pinsonneault (2010), emotions in general, when evoked by the announcement of a new IT system, relate to subsequent usage of that system. In our study, we do not find significant signals of *feelings* of fear (or other emotions), which Siponen et al. (2024) might explain by our focus on long-term, repeated behaviours. Overall though, more research is needed to clarify the conditions in which emotions in general, and fear specifically, play greater or smaller roles. Furthermore, we concentrated on danger-control processes, but following Lowry et al.'s (2023) recommendation, it may be relevant to study danger-control and fear-control processes together.

7. Conclusion

According to PMT, decision-makers adopt a focal coping behaviour in accordance with their appraisals of the focal coping behaviour and the focal threat. This paper clarifies that focusing exclusively on the focal threat and coping appraisals might not provide a comprehensive understanding of decision-makers' intentions to adopt the focal coping behaviour. We explore the decision-making process of restaurant

managers in relation to work misrepresentation behaviours. The interview narratives suggest that PMT accurately explains their choice to adopt the focal coping behaviour only when these decision-makers consider the focal coping behaviour legitimate and do not perceive significant related threats, alternative coping behaviours, or additional benefits. This qualitative study provides novel, clear insights into the boundary conditions of PMT that, in turn, inform our formulation of the RTCAF. This proposed framework includes focal threat and coping appraisals from PMT but also recognizes that the decision to adopt a focal coping behaviour is influenced by appraisals of alternative coping behaviours, competing and complementary threats, perceived legitimacy, and perceived additional benefits.

Declaration of use of "Generative Artificial Intelligence" technologies

During the preparation of this work, the authors used ChatGPT and Delos in order to improve readability and language of the work. After using this tool, the authors have revised and edited the content as necessary and assume full responsibility for the content of the publication.

CRediT author statement

Frank Goethals: conceptualization, investigation, formal analysis, validation, writing – original draft, writing – review & editing, visualization; Lies Bouten: conceptualization, investigation, formal analysis, validation, methodology, writing – original draft, writing – review & editing, visualization.

Acknowledgements:

We appreciate the thoughtful and relevant comments from Aurélie Leclercq-Vandelannoitte, Joao Vieira da Cunha, Christine Abdalla Mikhaeil, Elke Cabooter and Candace Jones, and the participants at the 30th CSEAR International Congress.

References

Ainsworth, R. T., & Hengartner, U. (2009). Quebec's sales recording module (SRM): Fighting the zapper, phantomware and tax fraud with technology. *Canadian Tax Journal, 57*(4), 719-761.

Alvesson, M., & Kärreman, D. (2007). Constructing mystery: Empirical material in theory development. *Academy of Management Review*, *32*, 1265–1281.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly, 34*(3), 613-643.

Aurigemma, S., & Mattson, T. (2019). Generally speaking, context matters: making the case for a change from universal to particular ISP research. *Journal of the AIS, 20*(12), 1700-1742.

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEO's information security behavior in SMEs: does ownership matter? *Systèmes d'Information et Management, 22*(3), 7-45.

Barlette, Y., & Jaouen, A. (2019). Information security in SMEs: determinants of CEO's protective and supportive behaviors. *Systèmes d'Information et Management, 24*(3), 7-40.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: a coping model of user adaptation. *MIS Quarterly, 29*(3), 493-524.

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly, 34*(4), 689-A3.

Bentham, J. (1780). *Panopticon* [Le Panoptique, traduit et publié par l'assemblé législative en 1791].

Berthevas, J. F. (2021). How protection motivation and social bond factors influence information security behavior. *Systèmes d'Information et Management*, *26*(2), 77-115.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly, 39*(4), 837-864.

Burns, A. J., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2023). Going beyond deterrence: a middle-range theory of motives and controls for insider computer abuse. *Information Systems Research, 34*(1), 342-362.

Busse, C., Kach, A. P. & Wagner, S. M. (2017). Boundary conditions: what they are, how to explore them, why we need them and when to consider them. *Organizational Research Methods, 20*(4), 574-609.

Chen, C., Zhang, K. Z. K., Gong, X., Lee, M. K. O., & Wang, Y. (2020). Decreasing the problematic use of an information system: an empirical investigation of smartphone game players. *Information Systems Journal, 30*, 492–534.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222.

Cromer, C. (2010). Understanding web 2.0's influences on public e-services: a protection motivation perspective. *Innovation, 12*(2), 192-205.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

Dambrot, S. M., de Kerchove, D., Flammini, F., Kinsner, W., MacDonald, G. L., & Saracco, R. (2018). Symbiotic autonomous systems. *IEEE*. Available at https://www.diva-portal.org/smash/get/diva2:1260812/FULLTEXT02.pdf.

Danermark, B., Ekström, M., & Karlsson, J. C. (2019). *Explaining society* (2nd ed.). Taylor & Francis.

Dang-Pham, D., & Pittayachawan S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. *Computers & Security, 48*, 281-297.

Dey, D., Ghoshal, A., & Lahiri, A. (2022). Circumventing circumvention: an economic analysis of the role of education and enforcement. *Management Science, 68*(4), 2914-2931.

Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: an application of Protection Motivation Theory. *Computers in Human Behavior, 60*, 508-513.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. (2000). A meta-analysis of research on Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

Fox, G., & Connolly, R. (2018). Mobile health technology adoption across generations: narrowing the digital divide. *Information Systems Journal, 28*, 995–1019.

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems, 115*(9), 1704-1723.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15–31.

Grimes, M., & Marquardson, J. (2019). Quality matters: evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems, 119*, 23–34.

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security, 17*(3), 276-289.

Hakansson, H., & Ford, D. (2002). How should companies interact in business networks? *Journal of Business Research, 55*, 133-139.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behaviour: a protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16.

Hegtvedt, K. A., & Johnson, C. (2009). Power and justice: toward an understanding of legitimacy. *American Behavioural Scientist, 53*(3), 376-399.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61-84.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18* (2), 106-125.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Gurpreet, D. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research, 25*(1), 111-136.

Huyberechts, P. (2024, September 26). Na doping nu een uitgekiend plan met startnummers. *Het Nieuwsblad*. https://www.nieuwsblad.be/cnt/dmf20240925_96478315

Ifinedo, P. (2012). Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviours: an empirical study. *MIS Quarterly, 34*(3), 548-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134.

Kirsch, L. J. (1997). Portfolio of control modes and IS project management. *Information Systems Research, 8*(3), 215-239.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67-94.

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security: an empirical study of intentional versus actual behaviour. *Information Management & Computer Security, 21*(1), 5-15.

Lai, F., Li, D., & Hsieh C.-T. (2012). Fighting identity theft: the coping perspective. *Decision Support Systems*, *52*(2), 353-363.

Laughlin, R. C. (1991). Environmental disturbances and organizational transitions and transformations: some alternative models. *Organization Studies 12*(2), 209–232.

Lazarus, R. S. (1991). Progress on a Cognitive–Motivational–Relational Theory of Emotion. *American Psychologist, 46*(8), 819-834.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping.* Springer.

Leclercq-Vandelannoitte, A., & Isaac, H. (2013). Technologies de l'information, contrôle et panoptique: pour une approche deleuzienne. *Systèmes d'Information et Management*, *18*(2), 9-36.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: an extended protection motivation theory perspective. *Decision Support Systems, 50*(2), 361-369.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed.) *Advances in experimental social psychology* (pp. 119-186). Academic Press.

Levi, M., Sacks, A., & Tyler, T. (2009). Conceptualizing legitimacy, measuring legitimating beliefs. *American Behavioral Scientist, 53*(3), 354-375.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring employees' IT compliance: carrot or stick? *Information Systems Research, 24*(2), 279-294.

Lowry, P.B., Moody, G.D., Parameswaran, S., & Brown, N.J. (2023). Examining the differential effectiveness of fear appeals in information security management using two-stage meta-analysis. *Journal of Management Information Systems*, 40(4), 1099-1138.

Lysyakov, M., & Viswanathan, S. (2023). Threatened by AI: analyzing users' responses to the introduction of AI in a crowd-sourcing platform. *Information Systems Research, 34*(3), 1191-1210.

Markus, M.L., & Benjamin, R.I. (1997). The Magic Bullet Theory in IT-enabled transformation. *Sloan Management Review, 38*(2), 55-68.

Matyn, J. (2022, February 9) Helft van gecontroleerde horecazaken betrapt op zwartwerk. *VRT.* https://www.vrt.be/vrtnws/nl/2022/02/09/helft-van-horecazaken-die-gecontroleerd-worden-op-zwartwerk-loop.

Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience: antecedents of cloud-based data backup. *Journal of Computer Information Systems, 55*(1), 83-91.

Mesgari, M., Mohajeri, K., & Azad, B. (2023). Affordances and information systems research: taking stock and moving forward. *The Database for Advances in Information Systems*, *54*(2), 29-52.

Miles, M. B., Huberman, A. M., & Saldana, J. (2020). *Qualitative data analysis: a methods sourcebook* (4th ed.). Sage Publications.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behaviour and protection practices. *The Journal of Consumer Affairs, 43*(3), 449-473.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behaviour: a meta-analytic review of Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Mingers, J. (2004). Re-establishing the real: Critical realism and information systems. In J. Mingers & L. Willcocks (Eds.), *Social theory and philosophy for information systems* (pp. 372–406). John Wiley & Sons.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366-2375.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42* (1), 285-311.

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A test of Protection Motivation Theory in the information security literature: a meta-analytic structural equation modelling approach. *Journal of the AIS, 23*(1), 196-236.

Nehme, A., & George, J. F. (2022). Approaching IT security & avoiding threats in the smart home context. *Journal of Management Information Systems, 39*(4), 1184-1214.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: a health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting against threats to information security: an attitudinal ambivalence perspective. *Journal of Management Information Systems, 38*(3), 732-764.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behaviour towards IS security policy compliance. In R. H. Sprague (Ed.), *Proceedings of the 40th Hawaii International Conference on System Sciences* (p 156), IEEE Computer Society Press.

Patton, M. Q. (2002). *Qualitative research & evaluation methods* (3rd ed.). Sage Publications.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551-567.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of a Protection Motivation Theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52*(3), 596-604.

Rogers, R. (1975). A Protection Motivation Theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. (1983). Cognitive and psychological processes in fear appeals and attitude change: a revised theory of protection motivation. In B. L. Cacioppoc, & L. L. Petty (Eds.), *Social Psychophysiology: a sourcebook* (pp. 153-176). Guilford Press.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection Motivation Theory. In D. Gochman (Ed.), *Handbook of health behaviour research: Vol. 1. Determinants of health behaviour: Personal and social* (pp. 113-132). Plenum Press.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Saldana, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). Sage Publications.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Qualitative studies in information systems: a critical review and some guiding principles. *MIS Quarterly, 37*(4), iii-xviii.

Schuetz, S. W., Lowry, P. B., Pienta, D. A., & Thatcher, J. B. (2020). Effectiveness of abstract versus concrete fear appeals in Information security. *Journal of Management Information Systems, 37*(3), 723-757.

Sewell, G., & Wilkinson, B. (1992). Someone to watch over me: surveillance, discipline and the just-in-time labour process. *Sociology, 26*(2), 271-289.

Silverman, D. (2000). *Doing qualitative research: a practical handbook*. Sage Publications.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: an exploratory field study. *Information & Management, 51*(2), 217-224.

Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2024). Protection Motivation Theory in information security behavior research: reconsidering the fundamentals. *Communications of the Association for Information Systems*, *53*, 1136-1165.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296–302.

Suchman, M. C. (1995). Managing legitimacy: strategic and institutional approaches. *Academy of Management Review, 20*(3), 571-610.

Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: a comparison and integration of alternative models. *Journal of Electronic Commerce Research, 14*(2), 183-200.

Tsai, H.-Y., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotton, S. R. (2016). Understanding online safety behaviors: a Protection Motivation Theory perspective. *Computers & Security, 59*, 138-150.

Tyler, T. R. (2002). Leadership and cooperation in groups. *American Behavioral Scientist, 45*(5), 769-782.

Van de Perre, S. (2014) Belastinggedrag en 'tax culture'. *Documentatieblad van het Ministerie van Financiën, 74*(2), 23-65.

Vance, A., Eargle, D., Eggett, D., Straub, D. W., & Ouimet, K. (2022). Do security fear appeals work when they interrupt tasks? A multi-method examination of password strength. *MIS Quarterly, 46*(3), 1721-1738.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198.

Vieira da Cunha, J. (2013). A dramaturgical model of the production of performance data. *MIS Quarterly*, *37(3)*, 723-748.

Weber, R. (2003). Editor's comments: still desperately seeking the IT artefact. *MIS Quarterly, 27*(2), iii–xi.

Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review, 14*(4), 490-495.

Whetten, D. A .(2009). An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and Organization Review, 5*(1), 29-55.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization, 16*, 304-324.

Witte, K. (1992). Putting the fear back into fear appeals: the extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Witte, K. (1994). Fear control and danger control: a test of the extended parallel process model. *Communication Monographs, 61* (2), 113-134.

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A Protection Motivation Theory approach to home wireless security. In D. Avison, D. Galletta, & J. I. Degross (Eds.), *Proceedings of the 26th International Conference on Information Systems* (pp. 367-380).

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*(4), 407-415.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioural intention in the workplace. An empirical study of Korean firms. *Information Technology & People, 26*(4), 401-419.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk-benefit appraisal approach, *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs, 43*(3), 389-418.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3-4), 180-197.

8. Appendix: Overview of settings in IS–PMT literature

Threat	Coping Behaviour	Gaps	References
Behaviour of employees			
S: Threat of data loss because of hard drive crash in old computer	S: Cloud based data backup	*Related behaviours: Backup on USB key* *Related threats: (-) 3rd party data theft*	Menard et al (2014)
S: Data theft because of not logging off computer	S: Information Security Policy Compliance: log off computers	*Related behaviours: Encrypt all files* Related threats: (+) Chance of getting sanctions	Johnston et al (2015)
S: Getting a virus via email	S: Secure (cautious) email behaviour	Related coping behaviours: 'Technical controls' as a control variable *Related threats: (-) Risk of not opening an attachment which should be read*	Ng et al (2009)
I: Students may plagiarise	S: Use of anti-plagiarism software	**Related behaviours: 'Some faculty members may adopt different, equally effective means to prevent Internet plagiarism in their classes' p 367** **Related threats: (-) Faculty 'expressed serious concerns that the commercial anti-plagiarism software vendors might misuse the materials submitted to check for Internet plagiarism' p 367**	Lee (2011)
I: Malware infections	S: Anti-malware software purchase by the company	*Related behaviours: Don't allow USB-keys; don't give users administrator rights* *Related threats: (-) Genuine files may also be blocked by the software*	Lee & Larsen (2009)
I: Spyware infections	S: Anti-spyware software use	**Related behaviours: 'safeguarding measure could be a behavior (e.g., updating a password) or an inaction (e.g., stop downloading freebies).' (Liang & Xue, 2010, p 405)** *Related threats: (-) Genuine files may also be blocked by the software*	Johnston & Warkentin (2010) Liang & Xue (2010)
I: Outsider gets access to confidential data	G: Take measures to protect information	*Related behaviours: Don't store confidential data* *Related threats: (-) Changing passwords increases chance of forgetting passwords and data inaccessibility*	Workman et al (2008)
Behaviour of citizens			
I: Internet security attack	G: Protective actions	Related behaviours: seeking help, avoidance (different models) *Related threats: (-) Risk of not having access to genuine files*	Chen & Zahedi (2016)
I: Risks associated with opening emails	S: Use of email screening software	Related behaviours: Email screening self-efficacy **Related threats: (-) email authentication services might lead to privacy issues**	Herath et al (2012)
I: Losing data from the computer	S: Backup behaviour	*Related behaviours: use a virus scanner* *Related threats: (-) Backup with confidential data can be stolen and data subsequently misused*	Boss et al (2015)
I: Malware infection	S: Anti-malware software use (Boss et al, 2015) S: Be careful when opening attachments (Warkentin et al, 2016) I: Desktop security behaviour (Hanus & Wu, 2016; Dang-Pham et al, 2015; Tsai et al, 2016)	*Related behaviours: Cautious behaviour when accessing files from the web; make backup* *Related threats: (-) Genuine files may also be blocked*	Boss et al (2015) Hanus & Wu (2016) Dang-Pham et al (2015) Tsai et al (2016) Warkentin et al (2016)
G: Health threat	S: Adopt healthcare wearable devices (Gao et al, 2015) S: Adopt mobile health	*Related behaviours: Adopt a healthy lifestyle* Related threats: (-) Perceived privacy risk	Gao et al (2015) Sun et al (2013)
G: Privacy risks	G: Refrain (Youn, 2009, Milne et al, 2009) G: Online secure behaviour (Cromer, 2010) S: Take privacy protection measures on social networking sites (Mohamed & Ahmad, 2012)	Related behaviour: Seek, Refrain (different models) *Related threats: (-) Threat that vendors cannot proactively contact you if they notice problems in the batch of which you bought a unit.*	Youn (2009) Milne et al (2009) Cromer (2010) Mohamed & Ahmad (2012)

Table A1: IS settings in which PMT was used as theoretical lens

Table A1 lists IS settings in which PMT has been used to explain the behaviour of employees (top half) and citizens (bottom half). Settings are characterized as G=General, S=Specific, I=Intermediate. The reason for this is that it illustrates that alternative, specific coping behaviours have been grouped into a general coping behaviour, and complementary specific threats have been studied implicitly in previous research that refers to general threats that comprise several complementary specific threats. In line with Willison (2006), we characterize threats/behaviours as specific if they fall within broader categories of threats/behaviours. The Threat and Coping Behaviour columns respectively show the threat and coping behaviour mentioned in the paper. The Gaps column illustrates how related threats and coping behaviours also could be relevant in other IS settings.

In the table, studies investigating the same threat have been grouped. A (+) indicates another threat that also motivates the coping behaviour (i.e., complementary threat), whereas (-) signals another threat that discourages the coping behaviour (i.e., competing threat). Factors in normal font have been at least partly addressed in the cited research; bold font signals factors mentioned by those sources but not addressed (e.g., limitations sections); and italics indicate factors invented by us to illustrate the conceivability of the related threats and coping behaviours in that research setting.