Trust and High Control: An exploratory study of Counterproductive Work Behaviour in a high security organization

Searle, R. & Rice, C

DOI 10.1080/1359432x.2024.2344870
ISSN 1359-432X
ESSN 1464-0643

Publisher: Taylor and Francis Group

EUROPEAN JOURNAL OF WORK AND ORGANIZATIONAL PSYCHOLOGY
https://doi.org/10.1080/1359432X.2024.2344870

Trust, and high control: an exploratory study of Counterproductive Work Behaviour in a high security organization

Rosalind H. Searle [a] and Charis Rice [b]

[a]Adam Smith Business School, University of Glasgow, Glasgow, Scotland, UK; [b]Centre for Trust, Peace and Social Relations, Coventry University Technology Park, Coventry, UK

ABSTRACT

High security organizations utilize a fine balance between control and trust to maintain stability. Drawing on qualitative interviews with managers and employees concerning three Counterproductive Work Behaviour (CWB) incidents occurring within a "high control" organization, we explore the impact of this trust-control dynamic on individuals' sensemaking, social relations and workplace behaviours. We explore Human Resource Management (HRM) control practices, contrasting levels of control (over and under-control), form (formal and informal), and consistency of control management, that variously destabilize the balance of trust and control. Framed by this dynamic, employees undertake CWB as a means of maintaining their trusting relationships, professional goals and well-being in an unpredictable workplace. We demonstrate the value of understanding the trust-control dynamic for CWB and identify potential lessons for prevention.

ARTICLE HISTORY
Received 2 February 2023
Accepted 2 April 2024

KEYWORDS
Counterproductive Work Behaviour; trust; control; Human Resource Management; prevention

Introduction

This paper explores Counterproductive Work Behaviour (CWB) within a high security, highly controlled, Critical National Infrastructure (CNI) organization. Specifically, it focuses on Human Resource Management (HRM) control practices and their impact on trust. Trust is generally accepted as a multi-faceted psychological state that shapes positive expectations (Robinson, 1996) and the willingness to accept vulnerability (Mayer et al., 1995). In workplaces, trust is derived from a combination of elements including the interpersonal (trusting key organizational actors such as leaders and colleagues), and the organizational and institutional systems and controls that provide assurance that the other party will act reliably in the individual's best interest (Weibel et al., 2016). HRM practices are important drivers of organizational trust, affecting both interpersonal and intergroup trust, and the effectiveness of controls (Gould-Williams, 2003). When trust and control levels are effectively managed in an organization, this tends to have positive effects, including highly committed, motivated and cooperative staff who understand and uphold organizational standards (Lumineau et al., 2023). CWB such as sabotage, abuse, stealing, ignoring safety procedures, breaches organizational controls through actions that "violate significant organizational norms" or "formal or informal organizational policies, rules and procedures" (Robinson & Bennett, 1995, p. 556), threatening the organization and its stakeholders, or both. They comprise intentional and unintentional action (Carpenter et al., 2021), and trust problems can play a role in their emergence (Searle & Rice, 2018).

CNI organizations operate in sectors such as government, and national security, providing essential services that enable functioning and safe societies (Rice & Searle, 2022[1]). These organizations operate more obviously than others at the behest of "good levels" of both trust and control (Lazányi & Danaj, 2022) due to the potentially damaging and widespread societal effects should these organizations fail or be compromised. Employees need not only to be trusted to deliver their role expectations, but also with access to sensitive resources, systems, and even classified materials. At the same time, these employees are required to adhere to legislation and stringent internal compliance processes which are, at least in part, designed to detect CWB and safeguard the trustworthiness of the organization and its workforce. CNI organizations thus face an interesting practical conundrum in how best to "balance" trust-control dynamics to foster trust, support effective organizational functioning, and prevent CWB (Vedel & Geraldi, 2022). There is also a theoretical puzzle that contributes to longstanding debate on the relationship between trust and control and its impact on organizational life should either be disproportionately in play (c.f. Long & Sitkin, 2018). While a fundamental, though often implicit, assumption for those working in a CNI organization is that they are trustworthy, denoted by their authorized status (Martin, 2023), paradoxically, these organizations' deliberate high control practices may also signal that employees are *not* trusted (Siebert & Czarniawska, 2020). This paradox can have important implications since trust shapes employees' job attitudes and behaviours to enhance task performance, job satisfaction, wellbeing, and organizational citizenship rather than CWB (Ozyilmaz et al., 2018). Perceived "over control" can potentially "crowd out" trust leading to performance and relational problems (Weibel et al., 2016).

Using empirical data from in-depth interviews with high security – hereafter "high control" - CNI employees and managers, this

CONTACT Rosalind H. Searle rosalind.searle@glasgow.ac.uk

paper explores different CWB incidents. First, it contributes to debates on trust and control through exploring their roles and dynamics in understanding and mitigating CWB, highlighting the particular role of HRM control practices. Drawing on social information processing (SIP) theory (Salancik & Pfeffer, 1978) and a constitutive understanding of organizational dynamics (Vedel & Geraldi, 2022), we consider social influences for individual and collective CWB, illustrating how trust is impacted by high control systems, and features in CWB. Second, we contribute to the literature on the competing reference groups that signal descriptive and injunctive norms to employees (Götz et al., 2019). This includes a deepening of understanding of unit-level CWB, particularly social processes of communication and sensemaking in local responses to HRM practices (Carpenter et al., 2021). We outline the role of local social contexts in filtering information and identifying significant cues, shared beliefs and cognitions (Morgeson & Hoffman, 1999). Finally, we suggest means to strengthen CWB prevention in a CNI context.

Trust and control

Extant research has examined the relationship between trust and control, specifically whether they are substitutes, i.e., having control negates the need for trust, or complements, i.e., having controls enhances trust (Weibel et al., 2016). Long and Sitkin (2018) dichotomize control mechanisms into formal (sanctioned codified directives and rules), and informal (emergent routines and relational norms, local ways of doing things). Collectively, controls are important in creating predictable workplaces, particularly when fairly implemented (Weibel et al., 2016). They support work co-ordination and co-operation, shape performance expectations and standards, resource and reward allocation, and act as monitors to ensure organizational goals can be accomplished (Long & Sitkin, 2018). However, when over-used relative to trust-based practices, controls can undermine or "crowd out" trust (Weibel et al., 2016). Conversely, trust can also facilitate practices that are exploitative, unethical, or risky (c.f. Skinner et al., 2014).

HRM practices and control

HRM practices communicate and enact organizational culture (organizational values, beliefs and assumptions), and organizational climate, managing behaviour codified in various practices (Rice & Searle, 2022). These practices affect employee attitudes and behaviours (Guest, 2017). HRM practices are important sources of organizational information, and can act as controls that influence employees' actions via espoused desired behaviours, rewards and sanctions (Carpenter et al., 2021). For CNI organizations, unique performance and reliability compliance and assurances are required, prioritizing security and controls to "certify" their trustworthiness through adherence to externally imposed safety and security restrictions.

Although HRM practices can be constructed, they require group-based sensemaking to form organizational climates that embed them (Bowen & Ostroff, 2004). Studies have distinguished two approaches: top-down led, compliance-focused "hard" practices which use extrinsic motivational practices and hierarchy to align employees' behaviour with the organization's; and "soft" practices which encourage employee voice and build joint management that promotes employee autonomy and often enhances multi-level trust (Guest, 1987; Truss et al., 1997). In CNI organizations, "hard" HRM practices may be particularly problematic since they can undermine a culture of trust and instead promote one of risk (Cregan et al., 2021); they reduce collaborative interactions that diminish the means to identify and air concerns. Further, "soft" collective HRM practices are important during periods of uncertainty, where collaborative, open communication environments should support the raising of CWB concerns (Rice & Searle, 2022).

HRM controls comprise four practices, including Snell's (1992) three: input, output and behaviour controls. *Input controls* codify organizational entry requirements including the desired competencies (knowledge, skills and abilities) that signal legal and ethical compliance. These controls extend through practices including probation, socialization (induction) and training that formally communicate organizational expectations and standards, and through the informal sharing of norms and values (van der Werff & Buckley, 2017). In certain CNI organizations like our case study, security "vetting" is a very intrusive input control with the duration and magnitude of pre-employment verification deterring many applicants (Lomas, 2021). Security level and "clearance" protocols are required for specific work tasks and progression (Berkelaar, 2014), and ongoing employment (Janczewski & Portougal, 2000). Vetting extends to personal financial arrangements and leisure time (e.g., holiday arrangements and destinations). *Output controls* concern objectives and desired outcomes, designed to motivate and set the quality of employee performance, formalized in reward and recognition, and performance management practices (Long & Sitkin, 2018). *Behaviour controls*, focus on *how* work should be achieved, codified in performance management, development and training practices (Weibel et al., 2016). In CNI contexts behaviour controls often comprise multiple passwords and security protocols and restricted work and working areas (Grawemeyer & Johnson, 2011). Additionally, *normative controls* (Weibel et al., 2016), are significant for organizational trust, as they enforce organizational norms and value congruence by signalling the desirable behaviours and the sanctions for deviation; this occurs formally such as through employment termination and via informal social influence or "peer pressure". Together, these HRM controls are important for CWB prevention (Carpenter et al., 2021).

Counterproductive Work Behaviour (CWB) as control violations

CWB, though variously defined, comprises organizational control-violating actions threatening organizations and their members' effectiveness, safety, or wellbeing (Robinson & Bennett, 1995). They include individually-targeted (CWB-I) activities (e.g., favouritism/ostracization, verbal and physical assaults), and organizational-focused (CWB-O) (production deviances like non-adherence to standardized practices; organizational property theft, and sabotage). Less overt forms include effort withdrawal (Götz et al., 2019; Spector et al., 2006). CWB can be intentional (e.g., effort directed at breaking systems) or

unintentional/accidental, and passive (e.g., ignoring others' CWB) rather than active (Searle & Rice, 2018).

Prior research shows individual antecedents including personality may explain CWB, linking CWB to the dark triad (machiavellianism, narcissism and psychopathy) (O'Boyle et al., 2012), or difficulties in self-regulation (Fida et al., 2015). Increasingly, however, CWB is regarded as multi-dimensional and dynamic, and as having different antecedents and motivations based within specific social contexts (Duffy et al., 2006; Spector et al., 2006). Thus while extensive study of intentional "bad apples" (e.g., O'Boyle et al., 2012) has emphasized the importance of input controls for CWB prevention, there is growing recognition of CWB's social and organizational roots. Liao et al's (2021) meta-analysis found CWB occurs where reciprocal exchanges between employees and the organization are disrupted, such as following perceived injustices, and is inhibited where employees feel valued and respected. Such work explains CWB through the lens of organization justice theory (Greenberg, 1990). Justice, in its different forms, is recognized as an important antecedent to trust, especially during organizational change, contributing to uncertainty reduction as well as normative commitment (Colquitt et al., 2012). In contrast, injustice is an important stressor, that can lead to organizationally directed-CWB (Fox et al., 2001). CWB has also been explained via psychological contract theory (c.f. Jensen et al., 2010); it views CWB as reactions to breaches in the "set of beliefs that guide how individuals understand the exchange arrangement between them and their employer" (Searle & Rice, 2018, p. 17). Psychological contracts provide expectations and consistency to organizational life and are closely linked to trust in the organization (Robinson, 1996). Psychological contracts can be ruptured through organizational changes that negatively impact on employees' worklife, such as changes to remuneration and rewards, the loss of trusted leaders, and revised goals and strategies that may contradict previous cherished ways of working (Searle & Rice, 2018). Changes to the psychological contract can thus trigger different forms of CWB such as withdrawal of effort or retaliatory behaviours that seek "payback" and to recoup a sense of control (Bordia et al., 2008; Fox & Spector, 2006; Kraak et al., 2024).

A particularly useful theoretical lens given our interest in how the social and organizational context of a CNI might frame trust, control and CWB, is that of social information processing (SIP) (Salancik & Pfeffer, 1978). SIP considers social influences on individual and collective behaviours. It identifies the role of local social contexts in unifying social cues, filtering information, and interactive sense-making, leading to shared beliefs and cognitions (Morgeson and Hoffman 1999). Control systems also shape social contexts and relations, for example requiring team-based processes or centralization, influencing individuals' use of formal versus informal controls, and the levels of task interdependencies. Some prior CWB research has examined unit-level interactive sensemaking (Carpenter et al., 2021), finding collective-CWB to be related to leaders' modelling of inappropriate and abusive actions, and colleagues sharing their negative attitudes. Contextual factors and their unit-level manifestations, however, remains under-examined in CWB (Götz et al., 2019). Specifically, social processes have been conceptualized as important in subtly shifting norms and reframing controls. These arise from peer observation and learning, and through superiors shaping sensemaking and motivating certain behaviours. Social influences comprise injunctive norms (perceptions of what others approve and disapprove of to gain social reward or avoid punishment), and descriptive norms (perceptions about whether others are actually engaging in normative behaviour themselves, and motivating actions for *that* context) (Ghosh, 2023).

Trust-control dynamics and the impact on CWB

The relationship between CWB, trust and control is clearly complex and given the salience of each in CNI organizations, this context is illuminating for examination of CWB. This study utilizes a qualitative case study and asks one main question: *How, if at all, does the trust-control dynamic play a role in CWB, and what are the implications for CWB prevention?*

Building on work that suggests trust may trickle across individual relationships and organizational levels (Wo et al., 2019), in our analysis we were attuned to how individual trust perceptions are borne out in multi-level trust perceptions and relations. In exploring three separate incidents of CWB, we illustrate how the trust-control balance can drive CWB in different ways, understanding of which can help inform preventative strategies (Kisling & Das, 2023). Prevention has been divided into five forms to explain and counter disease in a health context (Kisling & Das, 2023), which provides a useful metaphor for considering CWB prevention. Upstream efforts (*primordial prevention*) are designed laws and national policies to protect the entire population, while more targeted interventions limit exposure or boost immunity for susceptible groups to prevent disease onset (*primary prevention*). In an organizational context, these would include employee selection, organizational controls and awareness training. *Secondary prevention* involves early detection, quickly identifying and containing those infected, while *tertiary* efforts reduce disease severity and relapse, and *quaternary prevention* identifies those "at risk" due to related illnesses. Applied to CWB, these downstream foci include ongoing monitoring and close attunement to attitudinal or behavioural "red flags" that could signal CWB risk.

Methodology

Study context and CWB incidents

The research context is a high control organization comprising part of the UK's Critical National Infrastructure (CNI). The organization's 6000 employees all have national security clearance. The project funder secured an introduction to the organization. Following ethical and security clearance, organizational gatekeepers were briefed on the research aims and then asked to identify CWB incidents. Organizational gatekeepers thus collaborated in the research design, starting with the interpretation of these incidents as CWB. While this raises various epistemological and methodological issues, our approach was pragmatic and practically necessary (Riese, 2019). This study was predicated on access to organizational data concerning commercially sensitive critical incidents in a CNI organization. Nonetheless, the researchers worked with gatekeepers to

ensure the ultimate three incidents selected for analysis included potentially different underlying drivers and manifestations for academic knowledge generation.

In-depth interviews with leaders and employees (total interviews $n = 17$) explored both the organizational context and specific CWB incidents, supplemented by relevant organizational document review, including HRM and security paperwork, to understand CWB sequencing, context, and outcomes. Purposive sampling of individuals included those privy to each incident and those with unique or specialist insight into the organization, such as managers and employees in Human Resources and Security. Collectively, our interviews comprised senior, mid and non-management levels including from the two departments where these CWB incidents occurred.

Individuals were first made aware of the research by the security team and their manager. Verbal and written informed consent provided assurance that interviews would be undertaken only by the researchers, were completely voluntary and would be anonymized in reporting. All those approached agreed to participate. Workforce composition was reflected in our sample, being mostly (though not exclusively) white, long-standing, male employees (see Appendix 1). Interviews lasted approximately an hour comprising two sections: first, the organization's climate and culture, its structure and the HRM context, followed by, for those who were privy, a critical incident component (Flanagan, 1954) exploring events prior, during and after the CWB incident(s). We drew on the "timeline technique" facilitating more accurate recollection of complex events (Hope et al., 2013). Interviews were recorded and transcribed in full. To preserve interviewee anonymity, identifiers are used in reporting. Due to the sensitive nature of the research context, supporting data is not available.

Analysis

Our primary approach to transcript coding was inductive and "open" (Strauss & Corbin, 1998), assigning extracts of text to codes iteratively, viewing coding not as a linear process but as recursive and reflexive (Braun & Clarke, 2021). Nonetheless, given our wider focus on trust, organizational control, CWB and its prevention, we were primed to identify discourse in the interview transcripts that spoke to those issues, and we therefore to some extent included an element of deductive practice. Collectively, this could be considered to align with an abductive "phroentic iterative approach" that seeks to integrate inductive and deductive techniques to address practical problems and contribute to existing theory (Tracy, 2018). Notably in this respect, in understanding how CWB was dealt with across the case study incidents, our data analysis revealed different prevention logics, strategies and shortcomings that we felt could be conceptualized through reference to the modalities demarcated by Kisling and Das (2023) outlined above. Thus the Kisling and Das model emerged as a useful organizing framework for this aspect of our research question and, more widely, as a valuable way of thinking about prevention, to date underutilized in the CWB literature.

Interviews were coded using the software package "Nvivo". Through constant comparison and reflection on the possible links, we moved from inductive "first-order codes" to "second-order themes" (Brown & Coupland, 2015) until no new substantive observations or linkages occurred. This meant moving from numerous and broader descriptive codes to fewer, specific interpretive themes, arranging and rearranging these in an effort to respond to our research question (Tracy, 2018). The resultant coding was independently checked, verified or negotiated by the two authors in the interpretation and assignment to codes and wider themes; this recursive activity was undertaken following each interview transcript coding, and then again collectively on coding completion. The process was further strengthened by reflections and comparisons from each authors' field notes and memos made during data collection and the early stages of analysis. Our themes were also discussed with, and validated by, organizational gatekeepers and a project steering group through live project updates, feedback sessions and reporting. An illustration of the coding process is provided below in Table 1:

Throughout our analysis, we primarily focused on the individual level of analysis. However, as is common in qualitative research, we then compared and contrasted across these individual perspectives (across for example, teams, roles, managerial-non-managerial position), aggregated them, and derived patterns and anomalies that allow us to provide a collective account of CWB in its particular social context (Vogl et al., 2019).

Findings

Exploration of the CWB incidents reveals that while each incident was associated with an individual, closer examination

Table 1. Coding illustration.

Codes (First Order)	Theme (Second Order)	Illustrative Quote
• Trust and professional identity • Vetting as a signal of trust • Trust as a core organizational value • Breakdown in trust foundation and depleting impact on relationships	Trust as normative control of professional behaviour	"there is a general feeling here that if you have been given one of these [security passes] you are trustworthy, and you all work together and we trust each other and you do each other no harm".
• Response to CWB: Fear of HR over-reaction • Distrust and self-protection	Over-control: imbalance of control relative to trust	"It's interesting, when we have gone to talk to people . . . they distrust HR. I think because it sets off disciplinaries and grievances too regularly, or their perception is you are into some formal process very quickly".
• Local team climate as informal control • Dark side of trust • Re-framing of organizational values	Relational norms	"[we're] not always that effective at communicating. And I think sometimes this 'need to know' [only basis] culture where you blinker things off, gets to an extreme where people don't say anything".
• Hierarchy impacts on process control management • Organizational changes – trust/distrust of new leaders • Local managerial approach to process controls	Mixed messages: impact on controls	"I think a lot depends in terms of who line managers are and on their personal qualities in all honesty. You know some are very good and some may not be so professional".

reveals more pervasive unit-level CWB, manifested through disengagement in proactive security management, and control "workarounds", this was also associated with low trust of key actors specifically, HR. Social information sharing through injunctive and descriptive norms is apparent amongst colleagues which shapes and "localizes" risk attention and control compliance. Further, the findings suggest that where trust-control dynamics are not appropriately managed, this can pre-empt particular types of CWB. In incidents where participants perceived over-control from HR management regarding behavioural controls and sanctions (normative controls) (for example, incident 1), employees' sense of felt trust from managers is diminished, prompting CWB withdrawal at interpersonal, team, and organizational levels. In incidents where there is a perceived under-control of problematic individuals (for example, in incident 2), this can exacerbate existing team and managerial trust problems, and encourage interpersonal retaliatory CWB. When, in compensation, under-control swiftly pivots to over-control, this inconsistency is also trust diminishing. In incidents where hard HRM controls and ways to access rewards become opaque, organizational trust diminishes and in its place trusted colleagues' CWB becomes reframed as team-level OCB (for example, in incident 3). As illustrated below, a key cross-incident theme is the role of norms in the trust-control dynamic.

Incident 1: 'off-site loss'

The first CWB incident involved a long-standing employee's loss of a confidential and highly sensitive document off-site. It was found and returned shortly afterwards by a contractor; nonetheless it represented a serious security breach with significant organizational reputational threat. The employee's failure to initially report the incident, and their attempt to photocopy and replace the document was regarded as an attempt to cover-up their wrongdoings, with consensus among interviewees however, that their intention was never malicious, rather self-protective. Nonetheless, this individual's employment was terminated.

This individual's potential risk was generally acknowledged prior to the incident, as revealed by responses such as: "if it was going to happen to anybody, it would have been him" (I5). Such behaviour was part of a pattern of ongoing shortcomings that reveals secondary and tertiary prevention omissions (Kisling & Das, 2023):

> Because of the nature of the work on site we have strict health and safety on site … on at least two occasions he got into trouble for forgetting his cycle helmet or not having cycle lights on in the dark. It was just another example, now I think about it, of him not taking something seriously that everybody else takes seriously (I5).

Such behaviours were attributed to this individual's fundamental unsuitability for this CNI organization, illustrated by normative attitudes and behaviour starkly different to their colleagues:

> We are a little bit more engaged with what we do, and more positive in what we do … we are working at a one-off place and there is an element of, it's a privilege to have a specialised job, I don't think he got that. (I6)

This arguably also reflects a failure of input control and primary prevention shortcomings at the point of the individual's recruitment. Though aware, colleagues did not help to mitigate risk given their failures to raise concerns about non-adherence to security process controls:

> He worked in our team for a number of years, and we had mentioned that if he loses a password that's a drop everything and fix it thing … [but] I don't think we probably impressed upon him more how serious they [security breaches] were … because I wasn't his line manager I then didn't take it that I needed to further impress on him or start nagging him. (I6)

These colleague omissions constitute further unit-level CWB (Carpenter et al., 2021), and reveal unit descriptive and injunctive norms regarding security controls (Ghosh, 2023). Non-managers abdicate responsibility for reporting ongoing concerns to managers, and disengage from their "risky" colleague. Yet, the final employment termination was regarded by many as overly harsh, despite this history. Indeed reticence to report their behaviour appears reinforced by perceived over-control and unduly harsh HR disciplinary for minor breaches:

> When little safety things happen you don't mention them because you know there is going to be an overreaction … you can end up closing down entire facilities because somebody didn't do their shoelace up or something … you tend to think I am not going to mention that one. (I14)

When compared and contrasted against other CWB incidents, such comments reveal inconsistency in the organizational implementation of controls, a view employees and mid-level manager alike supported:

> It really depends on who you get on the end of the phone [with HR]. Sometimes I have been told, "it is entirely up to you". Sometimes, it must be done to the blueprint and you know, that's unnecessarily harsh and then the person's a bit disgruntled … It's very uncertain. You never really know what you are accountable for. (I14)

In conclusion, insufficient input controls – in so much as they are primarily competency rather than behaviourally and socially focused in this organization – partly explains the recruitment of an individual with poor role and organizational "fit", indicating primary prevention shortcomings. While the individual's vetting signalled their trustworthiness at organizational entry, their colleagues' daily work interactions did not confirm this designation. Seemingly, the individual's routine and predictable behaviours made this CWB preventable. Further, the positioning of reporting responsibility as a management task reflects a disconnect in secondary prevention in raising concerns, and signals a lack of felt trust for non-management employees. Previous inconsistent and formal reactions – "over-control" - by HR fuelled reporting anxieties. Specifically, this incident reflects breakdowns in employees' and mid-level managers' trust towards the HR team, arising from a perceived lack of benevolence and fairness (integrity). Perceived inconsistent control management (from under to over control) coupled with low trust in sanctions for control breaches (by HR), is associated here with unit-level withdrawal CWB.

Incident 2: 'sabotage'

Incident two involved the loss of a Removable Hard Drive containing sensitive information. After extensive searches by the organization's security teams, it was found unconcealed in the team manager's previously searched drawer. Although the perpetrator was not identified, general consensus was that someone had "planted" the missing drive there as an act of sabotage, or at least to avoid accountability. The organization's response was to formally control with written warnings to the entire team, and implement tighter security procedures (i.e., no one left alone in secure areas).

The interviews revealed a team with ongoing poor-quality relationships, and intra-team resentment towards those labelled as behaving counterproductively or withdrawing, yet with little normative management control, denoting primary, secondary and quaternary prevention shortcomings:

> Behaviours weren't as positive or strong in terms of teamwork and pulling together … people were getting frustrated with those that weren't actually delivering … individuals being disruptive to the team putting additional pressure on those ones who were trying to be supportive. (I7)

In the wake of this incident, some team members perceived deliberate sabotage of their new team manager, regarded by some as trying to covertly implement unwelcome radical changes. Given the legacy of continual organizational changes including leadership transitions, redundancies and removal of cherished rewards (reduced final pensions) – "shocks" that have been shown to be destructive to employees' psychological contract (Searle & Rice, 2018) – a malevolent agenda was perceived in the new leader's arrival. This created distrust towards the manager, which coupled with within-team discontent, provided the foundation for the incident, in the minds of some:

> Would I be surprised looking back at some of the behaviour, the dissatisfaction with some of the team members that may have acted and done something deliberately? Not fully surprised. (I7)

Organizations that are perceived to fail to fulfil their responsibilities tend to encourage retaliatory CWB from employees and breed team climates of incivility (Liao et al., 2021). Research shows that poor supervisor-supervisee relationships are important triggers of CWB, given the power differentials with supervisors controlling access to resources (Liao et al., 2021). The subsequent team-wide formal discipline precipitated declines in work motivation and organizational trust, revealing shortcomings in further CWB quaternary prevention, as one employee explained:

> There is a general feeling here that if you have been given one of these [security clearance passes] you are trustworthy, and you all work together and we trust each other and you do each other no harm. So, that was shattered. It had a, quite a bad impact on the team. You know de-motivational because they all felt that they were held guilty for something that they hadn't done. (I9)

The outcome includes the shame of perceiving one is distrusted (Skinner et al., 2014), which is intensified in a CNI organization since security vetting underpins one's professional identity (Rice & Searle, 2022). Similarly to incident one, the subsequent perceived "hardline" disciplinary and tightened security procedures were contrasted with other incidents where more lenient sanctions were used, and fuelled further feelings of injustice from inconsistent output controls as team members moved to other parts of the organization. These negative experiences became important anchoring events (Ballinger & Rockmann, 2010), with enduring further consequences for relationships between employees, their colleagues and leaders that cascade across the organization as colleagues move roles and teams.

To conclude, this incident shows the effects of both low trust (apathy, limited teamwork) and active friction between team members, and arguably *distrust* towards the new manager. Distrust is associated with pervasive negative perceptions and expectations, and a self-amplifying cycle of negative emotions and behaviours (Bijlsma-Frankema et al., 2015). This is alongside inconsistent process controls that could be exploited without explicit identification. Foundational to the event was poor team conflict management, which is central to primary, secondary and quaternary prevention. Concurrently, given a baseline of trust from organizational input controls of vetting and security passes that frame subsequent relational ties, this incident was particularly shocking as it was at odds with this context's normative idea of a "trusted professional". The output control of disciplining the entire team was arguably an overzealous reaction to organizational system failure, and signals a lack of benevolence from HR and security. This incident suggests that perceived under-control of problematic individuals, low interpersonal and intra-team trust and distrust in team management can be associated with interpersonally-directed retaliatory CWB, supporting existing research (Spector et al., 2006).

Incident 3: 'hoarding'

Incident 3 exemplifies the "stretching" and ultimately jeopardizing of security controls within a trusted team. A longstanding employee with prior history of similar behaviour accessed a secure area of a network for which they had no authorization, collecting large amounts of information in an online folder shared with team colleagues; it was not deemed malicious, but undertaken to support teammates' promotions. One interviewee explained:

> A way to progress, promotions, that has become unclear … changes to performance review, new software is coming in, it's all left people a bit frustrated … [the emailing of sensitive information] it was to help them [colleagues] with their promotion board. (I14)

This incident demonstrates the utilization of a trusted peer micro-network, despite its organizational security risks. It reveals a failure to monitor relapse of a known "threat", indicating tertiary prevention shortcomings. The motive features as an attempt to gain autonomy and clarity following a period of organizational change which affected important output reward controls. Interviewee perspectives reveal unit-level CWB, as colleagues were aware of the behaviour but the emergence

of injunctive norms (social reward from in-group inclusion for an often isolated and introverted team member) led to failures to raise concerns because of perceived benevolent intentions, but also the personal benefit derived from these resources:

> The whole jokey thing egged him on a little to be that person … that knows all the information … there was an opportunity there for him to have a joke and a laugh with people … I think it made him feel like it was normal and it was good. (I14)

Such comments demonstrate a breakdown of normative controls through team dynamics, rendering these antics acceptable and ultimately providing a sense of inclusion for this individual in this team.

Further, an important interview theme revealed it was not uncommon for inconsistent control communication at organizational entry:

> It could well be that when he first started the job someone went, "right you have got clearance … crack on, have a look where you want". They might really have just not said to him, "every time you go on the folder, this is only to be used for X Y Z, it's not here for this, it's not here for that". (I15)

The resultant ambiguity and omission of "folder surfing" as an explicit "red flag" security breach was seemingly reinforced through an in-employment training omission regarding process controls that reduced the means of primary prevention, as the following quote reveals:

> People shouldn't just "nose around" because they can … it was highlighted to us during training, but still I think that subtlety can be lost. (I12)

Importantly, the eventual identification of the behaviour was linked to the team merging with another group and the new manager being "far less tolerant of sharing things" (I14). This denotes inconsistencies in managerial utilization of process controls that impeded the effectiveness of tertiary prevention.

In conclusion, this incident illustrates how CWB emerged from shortcomings in all four control forms – input (recruitment, initial explicit induction training), output (reward processes), process (raising of security breaches), normative (managerial and peer tolerance of risky behaviours). These are linked to primary, secondary, tertiary and quaternary prevention failures. The incident juxtaposes the significance of seemingly positive trust and inclusion team dynamics with unit-level CWB. Distinct from the other two incidents, here, paradoxically, organizationally-directed CWB was a form of team citizenship. It reveals how deviant acts in a trusting and cohesive team can be rationalized when they serve the group (Bollmann & Krings, 2016). Whereas in incident one CWB involved an individual who did not identify with their role or the organization's high control culture, here the individual was highly identified, yet counter-intuitively unit-level injunctive norms regarded organizational rules as breakable (e.g., accessing folders only when strictly necessary for specific organizational tasks) where they violate the "greater good" (Dahling & Gutworth, 2017).

Discussion

A high security, highly controlled, Critical National Infrastructure (CNI) organization is a useful strategic context in which to explore trust, control and CWB. Specifically, we explored Human Resource Management (HRM) control practices, revealing contrasting levels of control (over and under-control), form (formal and informal), and consistency of control management, that variously destabilize the balance of trust and control. We propose that explanations of CWB must include attention towards not just organizational systems and practices that "build in" trust and control, but also local contexts and relational dynamics where such organization-wide practices are routinely challenged, negotiated, re-interpreted or undermined through everyday social interactions.

Trust-control and CWB

Our analysis demonstrates that formal controls, even in "high control" CNI organizations, are processed and made sense of through reference to local (unit) social contexts and norms. Thus it supports existing literature on the importance of social information and how it is collectively processed and "transferred" across interpersonal relationships and organizational levels, with tangible effects for workplace behaviours (Salancik & Pfeffer, 1978). We offer support to existing literature on the importance of situating CWB within a particular social context (Carpenter et al., 2021; Duffy et al., 2006), particularly that group dynamics are critical to advancing CWB understanding. Our incidents show that individual CWB can arise in contexts of collective "unit level" CWB where injunctive and descriptive norms (Ghosh, 2023) undermine formal security policies.

Further, we validate the importance of attending to how trust can emerge as an informal behavioural control that may actually facilitate CWB as team members seek to protect their position as trusted in-group members (Lumineau et al., 2023). In CNI organizations, controls comprise visceral, immersive experiences leading to distinct workplace identification and social norms amongst employees (Ashforth et al., 2023). But, paradoxically, stringent authenticating protocols can engender a climate of trust for those successfully vetted, creating psychologically "safe harbours" influencing whether employees raise concerns outside of their trusted team colleagues (Edmondson, 1999). This is reinforced by the role of informal norms (e.g., "one doesn't report on team members", "reporting creates unfair consequences"). Further, where HR managers (and managers more generally) are perceived to inconsistently deploy controls, oscillating between under-control of problematic individuals and over-control using rigid hierarchical structures and formal procedures, this communicates low employee trust, and increases the pull inwards towards trusted peer networks (Skinner et al., 2014). Inconsistent control management and their opaque applications creates multiple injustices bolstering collective CWB (Fox et al., 2001; Götz et al., 2019). Mixed messaging and perceived injustices have unintended consequences, enabling employees to feel justified in abdicating responsibility for raising concerns, particularly when "problem" individuals are already known to management in a strongly hierarchical organization (loss, incident 1 and hoarding, incident 3), and where inaction provides potential shared benefits (hoarding, incident 3). We show that withdrawal behaviours can, in this high control context, manifest

as specific withdrawal from risk monitoring and reporting, rather than more well-known behaviours counted more broadly as "working less" (see Spector et al., 2006). Further, CWB is exacerbated by organizational changes that escalate trust concerns, including imposing new managers (sabotage, incident 2), or informational asymmetry for progression (hoarding, incident 3).

Prevention implications

While strict input and output controls (primary prevention) are important in high security organizations, our findings suggest that more attention should be paid towards secondary, and tertiary prevention (Kisling and Das, 2023). A key means of doing this involves paying close attention to social information sharing, local norms and trust relations, how these may destabilize a "healthy" balance of trust and control (Vedel & Geraldi, 2022) and in turn facilitate CWB. It is clear from our study that CWB may be defined, perceived and identified in divergent ways between managers and non-managers, within and across teams, that open two-way dialogue on the topic could help address. In particular, co-orientation, a communication strategy to uncover and understand implicit contrasting perspectives and realities between individuals (Rice et al., 2021) may be useful as part of secondary prevention strategies. Further, an important omitted component of organizational control that could have signalled organizational trust lay in the identification and admission of apparent mistakes (Ozyilmaz et al., 2018). However, differences in attention and responses to errors by individual managers contributed to CWB (Götz et al., 2019). Unpredictable and unjust organizational experiences lead to repeated breaches of the psychological contract (Robinson, 1996).

Limitations

Our data may be subject to typical attributional errors that interviewees make in retrospectively making sense of past events (Weiner, 1985). The space limitations and security concerns of studying this particular CNI organization constrained the inclusion of further corroborating evidence, including from organizational documents and surveys. We cannot infer causation from our qualitative analysis, but propose that our findings highlight important issues related to trust-control dynamics and social conditions that are significant to understanding and mitigating CWB. Further study should test the generalizability of these findings, both in other high control organizations and beyond.

Conclusion

Drawing on qualitative interviews with managers and employees for three CWB incidents occurring within a "high control" organization, we demonstrate the value of understanding the trust-control dynamic for CWB. We uncovered collective withdrawal, "payback", and "passive" behaviours, that divert from organizational formal controls. Organizations can look to improve their resilience towards CWB through tiered prevention, moving away from solely mass pre-entry controls to real-time identification. This involves attunement to local social relations, particularly of trust, as well as identifying "at-risk" individuals.

Note

1. See NPSA website for further examples of CNI organizations: Critical National Infrastructure | NPSA.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The work was supported by the Economic and Social Research Council (ESRC) (ESRC Award: ES/N009614/1)-Centre for Research and Evidence on Security Threats (CREST).

ORCID

Rosalind H. Searle http://orcid.org/0000-0002-6052-7627

References

Ashforth, B. E., Caza, B. B., & Meister, A. (2023). My place: How workers become identified with their workplaces and why it matters. *Academy of Management Review*, amr.2020.0442. https://doi.org/10.5465/amr.2020.0442

Ballinger, G. A., & Rockmann, K. W. (2010). Chutes versus ladders: Anchoring events and a punctuated-equilibrium perspective on social exchange relationships. *Academy of Management Review*, *35*(3), 373–391. https://doi.org/10.5465/amr.35.3.zok373

Berkelaar, B. L. (2014). Cybervetting, online information, and personnel selection: New transparency expectations and the emergence of a digital social contract. *Management Communication Quarterly*, *28*(4), 479–506. https://doi.org/10.1177/0893318914541966

Bijlsma-Frankema, K., Sitkin, S. B., & Weibel, A. (2015). Distrust in the balance: The emergence and development of intergroup distrust in a court of law. *Organization Science*, *26*(4), 1018–1039. https://doi.org/10.1287/orsc.2015.0977

Bollmann, G., & Krings, F. (2016). Workgroup climates and employees' counterproductive work behaviours: A social-cognitive perspective. *Journal of Management Studies*, *53*(2), 184–209. https://doi.org/10.1111/joms.12167

Bordia, P., Restubog, S. L. D., & Tang, R. L. (2008). When employees strike back: Investigating mediating mechanisms between psychological contract breach and workplace deviance. *Journal of Applied Psychology*, *93*(5), 1104–1117. https://doi.org/10.1037/0021-9010.93.5.1104

Bowen, D. E., & Ostroff, C. (2004). Understanding HRM–firm performance linkages: The role of the "strength" of the HRM system. *Academy of Management Review*, *29*(2), 203–221. https://doi.org/10.5465/amr.2004.12736076

Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, *18*(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238

Brown, A. D., & Coupland, C. (2015). Identity threats, identity work and elite professionals. *Organization Studies*, *36*(10), 1315–1336. https://doi.org/10.1177/0170840615593594

Carpenter, N. C., Whitman, D. S., & Amrhein, R. (2021). Unit-level counterproductive work behavior (CWB): A conceptual review and quantitative summary. *Journal of Management*, *47*(6), 1498–1527. https://doi.org/10.1177/0149206320978812

Colquitt, J. A., LePine, J. A., Piccolo, R. F., Zapata, C. P., & Rich, B. L. (2012). Explaining the justice–performance relationship: Trust as exchange deepener or trust as uncertainty reducer? *Journal of Applied Psychology*, *97*(1), 1–15. https://doi.org/10.1037/a0025208

Cregan, C., Kulik, C. T., Johnston, S., & Bartram, T. (2021). The influence of calculative ("hard") and collaborative ("soft") HRM on the layoff-performance relationship in high performance workplaces. *Human*

Resource Management Journal, *31*(1), 202–224. https://doi.org/10.1111/1748-8583.12291

Dahling, J. J., & Gutworth, M. B. (2017). Loyal rebels? A test of the normative conflict model of constructive deviance. *Journal of Organizational Behavior*, *38*(8), 1167–1182. https://doi.org/10.1002/job.2194

Duffy, M. K., Ganster, D. C., Shaw, J. D., Johnson, J. L., & Pagon, M. (2006). The social context of undermining behavior at work. *Organizational Behavior and Human Decision Processes*, *101*(1), 105–126. https://doi.org/10.1016/j.obhdp.2006.04.005

Edmondson, A. (1999). A safe harbor: Social psychological conditions enabling boundary spanning in work teams. In R. Wageman (Ed.), *Research on managing groups and teams: Groups in context* (Vol. 2, pp. 179–199). Elsevier Science/JAI Press.

Fida, R., Paciello, M., Tramontano, C., Fontaine, R. G., Barbaranelli, C., & Farnese, M. L. (2015). An integrative approach to understanding counterproductive work behavior: The roles of stressors, negative emotions, and moral disengagement. *Journal of Business Ethics*, *130*(1), 131–144. https://doi.org/10.1007/s10551-014-2209-5

Flanagan, J. C. (1954). The Critical Incident Technique. *Psychological Bulletin*, *51*(4), 327–358. https://doi.org/10.1037/h0061470

Fox, S., & Spector, P. E. (2006). The many roles of control in a stressor-emotion theory of counterproductive work behavior. In P. L. Perrewé & D. C. Ganster (Eds.), *Employee Health, Coping and Methodologies* (Vol. 5, pp. 171–201). Emerald Group Publishing Limited. https://doi.org/10.1016/S1479-3555(05)05005-5

Fox, S., Spector, P. E., & Miles, D. (2001). Counterproductive work behavior (CWB) in response to job stressors and organizational justice: Some mediator and moderator tests for autonomy and emotions. *Journal of Vocational Behavior*, *59*(3), 291–309. https://doi.org/10.1006/jvbe.2001.1803

Ghosh, K. (2023). Employee-perceived 'motivation-enhancing HRM practices' and career ambition: Social subjective norms explain workplace deviant behavior. *Human Resource Management Journal*, *33*(4), 1074–1096. https://doi.org/10.1111/1748-8583.12503

Götz, M., Bollmann, G., & O'Boyle, E. H. (2019). Contextual undertow of workplace deviance by and within units: A systematic review. *Small Group Research*, *50*(1), 39–80. https://doi.org/10.1177/1046496418790044

Gould-Williams, J. (2003). The importance of HR practices and workplace trust in achieving superior performance: A study of public-sector organizations. *The International Journal of Human Resource Management*, *14*(1), 28–54. https://doi.org/10.1080/09585190210158501

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007

Greenberg, J. (1990). Organizational justice: Yesterday, today, and tomorrow. *Journal of Management*, *16*(2), 399–432. https://doi.org/10.1177/014920639001600208

Guest, D. E. (1987). Human resource management and industrial relations [1]. *Journal of Management Studies*, *24*(5), 503–521. https://doi.org/10.1111/j.1467-6486.1987.tb00460.x

Guest, D. E. (2017). Human resource management and employee well-being: Towards a new analytic framework. *Human Resource Management Journal*, *27*(1), 22–38. https://doi.org/10.1111/1748-8583.12139

Hope, L., Mullis, R., & Gabbert, F. (2013). Who? what? when? Using a timeline technique to facilitate recall of a complex event. *Journal of Applied Research in Memory and Cognition*, *2*(1), 20–24. https://doi.org/10.1016/j.jarmac.2013.01.002

Janczewski, L. J., & Portougal, V. (2000). "Need-to-know" principle and fuzzy security clearances modelling. *Information Management & Computer Security*, *8*(5), 210–217. https://doi.org/10.1108/09685220010356247

Jensen, J. M., Opland, R. A., & Ryan, A. M. (2010). Psychological contracts and counterproductive work behaviors: Employee responses to transactional and relational breach. *Journal of Business and Psychology*, *25*(4), 555–568. https://doi.org/10.1007/s10869-009-9148-7

Kisling, L. A., & Das, J. M. (2023). Prevention strategies. In *StatPearls [internet]*. StatPearls Publishing.

Kraak, J. M., Hansen, S. D., Griep, Y., Bhattacharya, S., Bojovic, N., Diehl, M.-R., Evans, K., Fenneman, J., Ishaque Memon, I., Fortin, M., Lau, A., Lee, H., Lee, J., Lub, X., Meyer, I., Ohana, M., Peters, P., Rousseau, D. M., Schalk, R., & Tekleab, A. (2024). In pursuit of impact: How psychological contract research can make the work-world a better place. *Group & Organization Management*, 10596011241233019. https://doi.org/10.1177/10596011241233019

Lazányi, K., & Danaj, A. (2022). Can trust be a factor of organisational safety and security? In T. A. Kovács, Z. Nyikes, & I. Fürstner (Eds.), *Security-related advanced technologies in critical infrastructure protection* (pp. 379–390). Springer Netherlands.

Liao, E. Y., Wang, A. Y., & Zhang, C. Q. (2021). Who influences employees' dark side: A multi-foci meta-analysis of counterproductive workplace behaviors. *Organizational Psychology Review*, *11*(2), 97–143. https://doi.org/10.1177/2041386620962554

Lomas, D. W. B. (2021). #forgetjamesbond: Diversity, inclusion and the UK's intelligence agencies. *Intelligence and National Security*, *36*(7), 995–1017. https://doi.org/10.1080/02684527.2021.1938370

Long, C. P., & Sitkin, S. B. (2018). Control–trust dynamics in organizations: Identifying shared perspectives and charting conceptual fault lines. *Academy of Management Annals*, *12*(2), 725–751. https://doi.org/10.5465/annals.2016.0055

Lumineau, F., Schilke, O., & Wang, W. (2023). Organizational trust in the age of the fourth industrial revolution: Shifts in the form, production, and targets of trust. *Journal of Management Inquiry*, *32*(1), 21–34. https://doi.org/10.1177/10564926221127852

Martin, P. (2023). *Insider risk and personnel security: An introduction*. Taylor & Francis.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.2307/258792

Morgeson, F. P., & Hofmann, D. A. (1999). The structure and function of collective constructs: Implications for multilevel research and theory development. *Academy of Management Review*, *24*(2), 249–265. https://doi.org/10.5465/amr.1999.1893935

O'Boyle, E. H., Jr., Forsyth, D. R., Banks, G. C., & McDaniel, M. A. (2012). A meta-analysis of the dark triad and work behavior: A social exchange perspective. *Journal of Applied Psychology*, *97*(3), 557–579. https://doi.org/10.1037/a0025679

Ozyilmaz, A., Erdogan, B., & Karaeminogullari, A. (2018). Trust in organization as a moderator of the relationship between self-efficacy and workplace outcomes: A social cognitive theory-based examination. *Journal of Occupational and Organizational Psychology*, *91*(1), 181–204. https://doi.org/10.1111/joop.12189

Rice, C., & Searle, R. H. (2022). The enabling role of internal organizational communication in insider threat activity – evidence from a high security organization. *Management Communication Quarterly*, *36*(3), 467–495. https://doi.org/10.1177/08933189211062250

Rice, C., Stanton, E., & Taylor, M. (2021). A communication toolkit to build trust: Lessons from Northern Ireland's civil society peacebuilders. *Voluntas*, *32*, 1154–1164. https://doi.org/10.1007/s11266-021-00376-0

Riese, J. (2019). What is 'access' in the context of qualitative research?. *Qualitative Research*, *19*(6), 669–684.

Robinson, S. L. (1996). Trust and breach of the psychological contract. *Administrative Science Quarterly*, *41*(4), 574–599. https://doi.org/10.2307/2393868

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal*, *38*(2), 555–572. https://doi.org/10.2307/256693

Salancik, G. R., & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. *Administrative science quarterly*, *23*(2), 224–253. https://doi.org/10.2307/2392563

Searle, R. H., & Rice, C. (2018). *Assessing and mitigating the impact of organisational change on counterproductive work behaviour: An operational (dis) trust based framework*. CREST. https://crestresearch.ac.uk/resources/reports/cwb-full-report/

Siebert, S., & Czarniawska, B. (2020). Distrust: Not only in secret service organizations. *Journal of Management Inquiry*, *29*(3), 286–298. https://doi.org/10.1177/1056492618798939

Skinner, D., Dietz, G., & Weibel, A. (2014). The dark side of trust: When trust becomes a 'poisoned chalice'. *Organization*, *21*(2), 206–224. https://doi.org/10.1177/1350508412473866

Snell, S. A. (1992). Control theory in strategic human resource management: The mediating effect of administrative information. *Academy of Management Journal*, *35*(2), 292–327. https://doi.org/10.2307/256375

Spector, P. E., Fox, S., Penney, L. M., Bruursema, K., Goh, A., & Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? *Journal of Vocational Behavior*, *68*(3), 446–460. https://doi.org/10.1016/j.jvb.2005.10.005

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2nd ed.). Sage.

Tracy, S. J. (2018). A phronetic iterative approach to data analysis in qualitative research. *Journal of Qualitative Research*, *19*(2), 61–76.

Truss, C., Gratton, L., Hope-Hailey, V., McGovern, P., & Stiles, P. (1997). Soft and hard models of human resource management: A reappraisal. *Journal of Management Studies*, *34*(1), 53–73. https://doi.org/10.1111/1467-6486.00042

van der Werff, L., & Buckley, F. (2017). Getting to know you: A longitudinal examination of trust cues and trust development during socialization. *Journal of Management*, *43*(3), 742–770. https://doi.org/10.1177/0149206314543475

Vedel, J. B., & Geraldi, J. (2022). How managers respond to paradoxical control-trust dynamics in interorganizational relationships over time: A constitutive approach. *Journal of Management Studies*, *60*(8), 2060–2090. https://doi.org/10.1111/joms.12846

Vogl, S., Schmidt, E.-M., & Zartler, U. (2019). Triangulating perspectives: Ontology and epistemology in the analysis of qualitative multiple perspective interviews. *International Journal of Social Research Methodology*, *22*(6), 611–624. https://doi.org/10.1080/13645579.2019.1630901

Weibel, A., Den Hartog, D. N., Gillespie, N., Searle, R., Six, F., & Skinner, D. (2016). How do controls impact employee trust in the employer? *Human Resource Management*, *55*(3), 437–462. https://doi.org/10.1002/hrm.21733

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological Review*, *92*(4), 548–573. https://doi.org/10.1037/0033-295X.92.4.548

Wo, D. X. H., Schminke, M., & Ambrose, M. L. (2019). Trickle-down, trickle-out, trickle-up, trickle-in, and trickle-around effects: An integrative perspective on indirect social influence phenomena. *Journal of Management*, *45*(6), 2263–2292.

Appendix 1: Participant Demographics

Interviewee Level	Department	Tenure	Gender
Non-manager	Science & Technology	27 years	Male
Non-manager	Science & Technology	4.5 years	Male
Non-manager	Science & Technology	9.5 years	Male
Non-manager	Commercial	12 years	Male
Non-manager	Security	3 years	Female
Non-manager	Security	9 years	Male
Non-manager	Security	16 years	Male
Mid-level manager	Science & Technology	16 years	Male
Mid-level manager	Science & Technology	12 years	Male
Mid-level manager	Science & Technology	10 years	Male
Mid-level manager	Commercial	20 years	Male
Mid-level manager	Security	13 years	Male
Mid-level manager	HR	19 years	Female
Senior manager	Communication and engagement	5 months	Male
Senior manager	Security	4 years	Male
Senior manager	HR	2 months	Male