The Enabling Role of Internal Organizational Communication in Insider Threat Activity – Evidence from a High Security Organization

Rice, C. & Searle, R.

Original citation:
Rice, C & Searle, R 2022, 'The Enabling Role of Internal Organizational Communication in Insider Threat Activity – Evidence from a High Security Organization', Management Communication Quarterly, vol. (In-Press), pp. (In-Press).
https://dx.doi.org/10.1177/08933189211062250

DOI 10.1177/08933189211062250
ISSN 0893-3189
ESSN 1552-6798

Publisher: SAGE Publications

Article

Management Communication Quarterly
2022, Vol. 0(0) 1–29

DOI: 10.1177/08933189211062250
journals.sagepub.com/home/mcq

'The Enabling Role of Internal Organizational Communication in Insider Threat Activity – Evidence From a High Security Organization'

Charis Rice[1] and Rosalind H. Searle[2]

Abstract

This paper explores the role of internal communication in one under-researched form of organizational crisis, insider threat – threat to an organization, its people or resources, from those who have legitimate access. In this case study, we examine a high security organization, drawing from in-depth interviews with management and employees concerning the organizational context and a real-life incident of insider threat. We identify the importance of three communication flows (top-down, bottom-up, and lateral) in explaining, and in this case, enabling, insider threat. Derived from this analysis, we draw implications for communication and security scholars, as well as practitioners, concerning: the impact of *unintentional* communication,

[1]Centre for Trust, Peace and Social Relations, Coventry University Technology Park, Coventry, UK
[2]Adam Smith Business School, University of Glasgow, Glasgow, UK

Corresponding Author:
Charis Rice, Centre for Trust, Peace and Social Relations, Coventry University Technology Park, 5 Coventry Innovation Village, Cheetah Road, Coventry CV1 2TL, UK.
Email: charis.rice@coventry.ac.uk

the consequences of selective silence and the divergence in levels of shared understanding of security among different groups within an organization.

Keywords
crisis and risk management, employee misconduct, interpretive case study, organizational communication

Organizational communication is a central topic in the crisis communication literature. Coombs's (2007) Situational Crisis Communication Theory (SCCT) is a significant contribution that builds on attribution theory. SCCT dichotomizes crisis into three types: victim (e.g. natural disasters), accidental (e.g. technical error) and preventable (e.g. organizational misdeed); with each type progressing the level of accountability that is likely to be assigned to the organization by various stakeholders (Coombs, 2007; Denner et al., 2019). The SCCT model connects these crisis types with appropriate external communication strategies that organizational leaders can utilize, after stakeholder safety and ethics have been addressed, as a way of containing the reputational risks that typically follow crises (e.g. *denial, diminish, rebuild*).

An associated but less-developed area of research focuses on the role of *internal* organizational communication in mediating stakeholder reactions – namely, those of employees (Kim et al., 2019). However, a paucity of attention has been paid to the role of internal organizational communication in *contributing to* a crisis in which the organization is the victim; one such exemplar is the crisis that can arise from insider threat. This critical omission is the focus of this paper. The topic can be situated within the communication framing element of SCCT to enable examination of how the construction of messages influences how audiences understand and interpret a crisis. As Coombs contends: 'Frames in communication help to shape frames in thought' (2007, p.167). The SCCT argues that the framing of organizational crisis messaging – for example, managers' use of certain words, their focus and selection of information – can cue stakeholders towards a particular and desired interpretation. While SCCT, and much other crisis communication theory, offers communication strategies to manage a crisis once it transpires, in this paper we examine whether, and how, an organization's internal communication environment affects the (mis)behaviour of employees, since such behaviours may themselves constitute a crisis and reputational risk for the employing organization. We seek to understand if, how, and in what ways communication shapes the *emergence* of one particular kind of threat, that from 'insiders'. Through such attention, we expand and nuance crisis communication theory, by extending understanding of internal communication in crisis development.

The paper is structured as follows. First, we review pertinent literature to outline the theoretical background to this study, culminating in our research question. Then we elucidate the research context and our methodology. Next, we present and then discuss our findings. Finally, we conclude by identifying implications for theory, practice and further research.

Literature Review

Insider Threat as a Form of Organizational Crisis

Insider threat refers to danger from individuals with privileged levels of access to an organization's resources due to their internal position in the organization (Nurse et al., 2014, p. 214), such as employees, contractors or trusted third parties (Searle & Rice, 2018, p. 14). Crisis concerns 'a specific, unexpected, non-routine event or series of events that creates high levels of uncertainty and a significant or perceived threat to high priority goals' (Sellnow & Seeger, 2013, p. 7). Two main categories of insiders are evident – malicious insiders, who intentionally undertake wrongdoing for some kind of gain (e.g. financial), and non-malicious, or accidental insiders, who unintentionally harm the organization (e.g. through oversight) (Nurse et al., 2014). This distinction has some synergy with SCCT's crisis types of accidental (unintentional) or preventable (sometimes intentional) crises that emerge from stakeholder behaviour, alongside victim crisis in which an organization is attacked by internal or external agents beyond its control. In terms of insider threat, Searle and Rice (2018, p. 14) demarcate 'passive threat' as disengaged employees, who withdraw their full effort and attention from work tasks or whose inaction towards colleagues facilitates, or tacitly condones, an insider's behaviour. Thus, taken from a multi-level perspective (i.e. the role of the individual within the broader organization), insider threat presents an important context to study crisis communication through challenging the boundaries separating victim, accidental and preventable crisis types. For example, while Coombs (2007) suggests that rumour and workplace violence comprise the victim category – where an organization has only weak attributions of responsibility and thus risks mild reputational threat – a multi-level insider threat lens considers the workplace environmental triggers for these harmful employee behaviours. Through expanding explanations for employee deviance, Searle et al. (2017) contrast individual 'bad apples' with team or organizational level typologies that demonstrate the impacts of cultures, climates, leadership and relationships in producing 'bad barrels' or even 'bad cellars'. The #MeToo Movement has graphically shown the severe reputational threat to organizations that can follow from facilitating or ignoring the emergence of harmful norms, behaviours and communication practices.

Given the conceptual similarities, insider threat can be positioned as a form of potential, or actual, organizational crisis. A significant proportion of insider threat research focuses on technological determinants and implications, including monitoring of employees' cyber activity (D'Urso, 2006; Legg et al., 2013). Studies have largely focused on individual characteristics – psychological, behavioural and social – associated with distinct insiders. This focus includes personality traits of narcissism, Machiavellianism and psychopathy; behaviours, notably impulsivity and aggression; and poor-quality social relationships (e.g. Legg et al., 2013; Shaw et al., 1998). Such focus concerns the influence of deviant individuals within an organization, rather than examination of how a particular organization's working environment can negatively affect an otherwise 'good' employee and trigger insider threat behaviour. A few exceptions have attempted to provide a comprehensive framework to explain insider threat that incorporates individual, social, and organizational factors (e.g. Legg et al., 2013; Nurse et al., 2014; Searle & Rice, 2018; Whitty, 2021). Most recently, Knight and Nurse (2020) developed a framework for effective external corporate communication after cyber security incidents. Yet there remains a relative blind spot regarding the connections between internal organizational communication and insider threat in either the communication or the security literature.

Communication Environment, Responding to Risk and Voicing Concern

This research gap remains despite prior study indicating a wide range of internal organizational communication impacts, including employee job satisfaction and engagement, workplace relationships, organizational culture, organizational productivity, security and crisis (e.g. Men & Bowen, 2017; Taylor & Bean, 2019). Examination of the role of communication in insider threat thus involves attention toward both organizational culture (values, beliefs and assumptions that characterize an organization) and organizational climate (behavioural evidence that creates meanings concerning the various policies and practices) (Schneider et al., 2013) pertaining to security. For example, open organizational communication environments, which value employee input and demonstrate concern for employee interests, have been linked to organizational citizenship behaviour (OCB) (Walden & Kingsley Westerman, 2018). OCB includes voluntary protective security actions such as reporting a colleague's organizationally threatening behaviour to leaders (Morrison, 2014). Within safety critical contexts, silence about known risks can escalate threat, making employee voice critical to crisis prevention.

Bottom-Up Communication. Employee voice is central for internal whistleblowing (Skivenes & Trygstad, 2010) – the raising of concerns internally

about a problematic issue or behaviour witnessed within an organization to organizational leaders. 'Speaking up' behaviour within one's employing organization indicates that individuals feel psychologically safe (Edmonson, 1999), identify with the organization, care about interpersonal work relationships and feel empowered (see Morrison, 2014, for a review). Critically, employees must perceive the chances of retaliation for such action as low (Gravley et al., 2015). In participatory, rather than authoritarian, cultures, bottom-up communication also involves proactive problem identification (Bisel & Arterburn Adame, 2018; Mao & DeAndrea, 2018). Extant research indicates that, although time intensive, an inclusive bottom-up approach to communication enables organizational agents to identify dissent and build consensus and a sense of community amongst stakeholders (Lewis et al., 2001). Conversely, employees often remain silent on workplace concerns out of resignation towards the status quo ('acquiescent silence'), to protect themselves ('defensive silence') or to protect others ('pro-social silence') (Van Dyne et al., 2003, p. 1359).

Top-Down Communication. Leaders influence a host of organizational and employee level outcomes and meaning-making processes (Fairhurst & Connaughton, 2014), including safety behaviours (Clarke, 2013). Leadership may be defined, for example, by personal attributes, formal position or style (Eglene et al., 2007). Seeger and Ulmer's (2003) taxonomy of leaders' communication-based responsibilities includes espousing moral values, information about organizational operations and being open to signs of problems (p. 59). Leaders' reluctance or lack of capability to discuss complex matters of ethics and values with their employees can create norms that restrict or re-direct information flows (Seeger & Ulmer, 2003). Leader communication affects the formation of organizational culture, as well as the coherence of organizational climate across employee groups and organizational levels (Schneider et al., 2013). Research shows employees will be responsive to risk when they are able to access risk information and formal training, but their recognition of hazards also requires continual reinforcement through leadership modelling (Ford & Stephens, 2018). Knowledge sharing is enhanced where managers signal a willingness to act on employees' inputs (Detert et al., 2013) thus demonstrating that they are trusted (Nerstad et al., 2017). Further, employees receiving dialogic communication from leaders which is 'information rich' are likely to be satisfied in their jobs and inclined to work towards the organization's collective interests (Men, 2014). Certain organizational leaders may be particularly influential in this respect. For example, the communication of Human Resource leaders sends powerful key values and trustworthiness signals about the organization, which line managers can then reinforce (Searle, 2018).

Lateral Peer-to-Peer Communication. Nonetheless, while leaders may set the tone of the communication environment, this tone can be reinforced, challenged and negotiated by individual employees and teams. Individuals, both consciously and unconsciously, learn from their direct experiences and through interacting with their colleagues about how to behave and communicate, and this extends to deviance norms (Robinson et al., 2014). Indeed, a leader-centric view of organizational norm setting has been challenged, with recent study revealing how similar or lower-ranking individuals are the most accurate and preferred sources of social norm information (Dannals et al., 2020).

Given empirical endorsement of the relationship between work behaviour and internal organizational communication, in this study we address one overarching research question: *What role, if any, does internal organizational communication play in insider threat behaviour?* The next section outlines our research context, followed by our methodology.

Research Context

This case study involves a high security organization comprising part of the UK's critical national infrastructure (CNI). CNI organizations provide essential services that enable functioning and safe societies (e.g., see *CPNI*)[1] and therefore insider threat activity in these organizations may have wide societal consequences. However, given the focus on insider threat – rather than the organization per se – and the exploratory nature of the research question, our case study can be defined as instrumental (Stake, 1995). The organization is a relatively closed system, having limited external permeability and operating with very strict procedures and controls (Men & Bowen, 2017). To start and maintain their employment, all employees require various levels of national security clearance (vetting) that can be removed if concerns about one's personal or professional conduct are raised. The specific insider threat incident we examined is outlined later in the 'Findings - Critical Incident Overview' section.

Methodology

Data Gathering

Data collection comprised in-depth interviews and supplementary review of Human Resource (HR) and security documents. We chose in-depth qualitative interviews as our main data collection method because we were interested in the first-hand perspectives of individuals with unique insights. Before gathering data, the researchers' project plan and data collection approach underwent rigorous ethical review from their institution and the research funder, ultimately resulting in ethics clearance. In advance of data gathering, the two researchers gained appropriate security clearance, and they were

accompanied for the duration of their time on site by a security representative, with the exception of the interviews themselves.

Due to the understandable security sensitivities of this organization, insider threat incidents with potential for further exploration were first identified by the organization's security leaders and then discussed with the researchers. Selected cases were then collaboratively chosen because they represented, at face value, seemingly distinct types of insider threat comprising potentially different underlying causes and motivations that the researchers thought could be explored further (see Nurse et al., 2014), and those the organization's leaders believed would provide important organizational learning. Access to interviewees was facilitated by the security lead to ensure that those being interviewed were clear they had authority to talk to the researchers about these events. We therefore must acknowledge that, to some extent, the organization's gatekeepers were actively involved in the design of the research, starting with the interpretation of the incidents as 'critical'. While this raises various epistemological and methodological issues (see limitations section), the rationale for this approach was twofold. First, practically, as is common in qualitative research (e.g. Riese, 2019), our study was predicated on examining commercially sensitive critical incidents. Organizational gatekeepers are those who are privy to, and who can facilitate access to, sources of organizational data; we therefore recognized that our study must deal with topics considered relevant and potentially impactful to these individuals who act as brokers to the wider organization. Second, these organizational gatekeepers have specialized knowledge of the organization and which members could assist with our key informant purposive sampling (Patton, 2015; Payne & Payne, 2004). Key informants are individuals who, due to their social positions, have extensive or specialist knowledge about 'other people, processes or happenings' that makes them valuable information sources (Payne & Payne, 2004, p. 135). We wanted to collect and compare different perspectives from: (1) individuals with direct knowledge of the insider threat incidents (e.g. those implicated as 'insiders', their co-workers and team members, line managers, security specialists), and (2) individuals in the organization who represented different professional expertise and roles, as well as distinct departments, work groups and place in the hierarchy. This approach enabled a strategic but relatively comprehensive capture of both the particular insider threat incident and wider experiences of the organization, and illuminated important areas of convergence and divergence between individuals and groups (see findings section).

Accordingly, individuals were selected for face-to-face interview[2] over a two-week period at the organization's premises. Interviewees included three senior managers with oversight of the organization, two mid-level managers and one non-manager selected for their specialist experience/closeness to the case (HR, security and communications), and four mid-level managers and six non-managers with direct experience of the insider threat cases in the two

departments where insider threat had occurred (commercial operations and science and technology). The latter group included one 'insider' (who we term here the Subject of Interest – SOI), co-workers, team leaders and pertinent security staff. This sample of 16 individuals[3] broadly reflected the composition of the organization's workforce, comprising mostly (though not exclusively) white males and longstanding employees (average tenure across this sample is 11 years – see Appendix A). All interviews lasted approximately 60 minutes and were audio-recorded and transcribed in full.

Our interviews comprised a semi-structured approach covering two distinct areas – general and specific *context* and the *critical incidents* (selected insider threat cases) – with the focus and questioning adapted to the individual's particular role and experience. All interviews commenced with standard questions pertaining to individuals' job roles and basic work histories. We then focused on *context setting,* eliciting perceptions and experiences of the organization's culture and climate (e.g. organizational ethos and values; structures and leadership; control systems and rules; the organization's different departments and teams; employee relations, communication and engagement; HR, reward and disciplinary processes) and the meanings employees derived. Further probes explored the nature and exchange of communication. For relevant individuals, we used a *critical incident* focus (Flanagan, 1954) in considering events that led up to the insider threat case as well as what occurred during and following the incident. This approach was inspired by the 'timeline technique' that facilitates complex event recall (Hope et al., 2013). Reported quotes are anonymized to preserve respondents' confidentiality, using identifiers that range from I4 to I20.

In addition, security and HR documentation for the insider threat cases was collected. These materials included disciplinary letters, interview transcripts with the SOI, investigation reports and organizational/HR policy documents. Annual engagement survey results were also reviewed. Due to confidentiality restrictions, we cannot report this data here, nor did we systematically analyze this data. Instead, it was reviewed at a first pass level with relevant sections identified that informed our understanding of the research context (Bowen, 2009). These insights also informed specific interview probes. For example, survey results indicated consistently low satisfaction levels regarding organizational communication – this insight was used to probe *what* was or was not satisfactory regarding organizational communication, as well as how employees communicated with each other and their managers. Reference to such documentation also enabled cross-checking of our own and interviewees' understandings of organizational processes and how the critical incidents unfolded and were handled. These cross-checks increased the validity of our analytical interpretations (Whittemore et al., 2001). Other interview probes were informed by relevant research and theory, including the key themes outlined in our literature review.

Interview Analysis

Analysis of our interviews was informed by an interpretive framework, leaning on sensemaking and Interpretative Phenomenological Analysis (IPA) traditions. Sensemaking is a cognitive process that occurs as individuals search for meaning around events and experiences particularly when events disrupt routine organizational functioning, such as crisis or insider threat cases (Brown et al., 2015; Kim, 2018). To employ sensemaking, therefore, means attending to how individuals enact contexts and select meanings from their environment (Wieland, 2020, p. 468). These selections can reveal perspectives on personalities, roles, power relations, and normative expectations that are critical for interpretive analysis. Through our use of the timeline questioning technique (Hope et al., 2013), antecedents, mediators and consequences of insider threat could be more easily identified for subsequent analysis (this paper primarily reports on antecedents and mediators). Similarly, IPA prioritizes detailed accounts of individuals' lived experience, illustrated in their own words and reproduced by the researcher to critically consider 'what it means' to express specific feelings and concerns about a particular situation (Larkin et al., 2006, p. 113).

Practically, we broadly mirrored Braun and Clarke's (2006; 2020) four stages of reflexive thematic analysis: data familiarization, initial code generation, theme generation and review and defining and naming themes. Interviews were coded using the NVivo software package. The primary coding approach was open coding (Strauss & Corbin, 1998) assigning tentative codes to sections of data that captured interviewee reflections and discourse on pertinent issues relevant to our research question. 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. The resultant coding was independently checked, verified or negotiated by the two authors in the interpretation and assignment to categories 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 author's field notes and memos made during data collection and the early stages of analysis. Specifically, we drilled into areas of convergence and divergence to examine interpretations, patterns and differences across these interviews, thereby increasing analytical credibility.

Findings-Critical Incident Overview

As part of our wider insider threat study, three cases of insider threat were selected and investigated; due to space constraints, only one is

presented here, chosen for its communication themes (for others, see Searle & Rice, 2018). This critical incident involved a longstanding non-management employee (SOI) who had, without reason or authority, accessed top-secret documents from the organization's computer network, hoarded them, and in some instances, shared them with team colleagues. This was a breach of the organization's IT acceptable use policy and its 'need to know' principle, both of which are designed to ensure employees only access information that is both directly required for their work duties and fits their security clearance level. Given the high security status of the organization as part of critical national infrastructure, information is shared with the fewest people possible. As one interviewee reflected:

> Potentially … people accumulate information they didn't need to know in the course of their job role … security, they have to worry about things like spying, in a worst-case scenario. Obviously that is very rare but they do have to consider that possibility. And that's why the 'need to know is applied. (I13)

Employees' surfing, hoarding and sharing of cyber-based information can be problematic for organizations generally. These activities have the potential to compromise security, breach data protection, create organizational inefficiencies through slowing and cluttering systems and may distract employees, making them less productive (Neave et al., 2020). While the insider threat case we focus on in this paper reflects senior management/organizational policymakers' ideas of a critical and problematic incident, as we detail below, there was a strong consensus across all of those interviewed (managers and non-managers, including the SOI) that such behaviour was problematic for organizational security.

HR and security documents revealed that these breaches occurred over a seven-month period, averaging 371 files accessed each month. Following this discovery by a manager, an official investigation was launched, revealing the SOI's prior warnings for similar information hoarding. When confronted, the SOI initially justified their actions as 'natural curiosity', but swiftly accepted the actions as errors. The formal disciplinary investigation recorded a motivation to obtain a 'bigger picture' of the organization. While the SOI was aware of their hoarding actions, they confined their subsequent document access to assisting team members' work and promotion applications. Following Nurse et al.'s (2014) typology, this incident can be classified as an intentional but non-malicious threat. The SOI apologized and demonstrated a change in their subsequent behaviour. The disciplinary investigation found this was 'gross misconduct' necessitating a final written warning, with a permanent HR record, and ongoing random cyber-security checks.

Thematic Findings

We present our thematic findings under two macro headings: constraints to bottom-up communication, and constraints to top-down communication that together, we propose, act as enablers of insider threat behaviour.

Constraints to Bottom-Up Communication

Significantly, critical incident reflections from the SOI's team indicate that they were aware of the SOI's unusual cyber activities. Five wider organizational context factors appeared to collectively restrain the sharing of security concerns with leaders who could have proactively intervened. Instead, within the team, the SOI's behaviour was (re-)framed as benign, and remained so until notification of an official security incident rendered this characterization unsustainable.

Lateral Communication as a Constraint to Reporting. An integral facet of the flow of bottom-up communication regarding the critical incident involved the lateral communication and relationships between colleagues. With hindsight, team members recognized that they had encouraged these hoarding activities, particularly as the information collected and shared by the SOI had material benefits in assisting their promotion applications or general work. Co-workers described the SOI's actions as team (rather than organizational) citizenship behaviours which significantly filled an information vacuum that arose following changes to promotion criteria. They agreed the SOI was a quiet and introverted person, somewhat awkward in their social interactions; subsequent professional support revealed an autistic spectrum diagnosis. Team members regarded the SOI as a valuable information provider, reinforcing this social position through in-team jokes and banter. One mid-level manager explained:

> The whole jokey thing has egged him on a little bit to be that kind of figure who knows all the information …We should never have been accepting those type of jokes sustained over years of him working here … it made him feel part of a team I think … because he's such a quiet person you know 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).

Colleagues were aware of ongoing similar security breaches but in acknowledging the personality 'quirks' of this individual who struggled socially and had non-malicious intent, enacted a protective, pro-social silence (Van Dyne et al., 2003). Team members, including the SOI, reflected that these activities were problematic and risky for security, indeed I14's discourse '*like* it was normal and good' implies the behaviours were, in fact, the opposite (e.g.

see López-Couso & Méndez-Naya, 2012). These jovial and inclusive social team dynamics and benefits implicitly suppressed organization-level security concerns. Concurrently, through various comments, colleagues acknowledged the SOI's security vulnerability: 'Of anybody in the team … I would probably say that it [an insider threat] was going to be him' (I14).

Fear and Distrust of HR. An important contributing factor to this incident arose from the climate of fear regarding HR, with their heavy-handed and inconsistent approach creating a more general suppression in raising colleague-related security concerns. Interestingly, this was an issue most deeply reflected on by interviewees with management roles. A senior manager explained: 'they [employees] 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' (I19). Further, mid-level managers indicated inconsistencies in HR processes, as one explained:

> 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)

While mid-level line managers' hesitancy was also related to dealing with the aftermath of HR discipline, including disgruntlement within their teams, HR representatives themselves saw things differently. HR interviewees perceived unwillingness, but also some incompetence, in managers' responses to counterproductive work behaviour. One senior HR manager explained:

> All of the line management would generally expect HR to take a significant role in any [disciplinary] process … that's come out of our leadership assessments that we just don't have managers equipped to work through those processes themselves … it's kind of like, 'here you go, this is what happened, can you please discipline my employee and send him back once you have finished?' (I20)

Management Communication, Management Accountability. Senior managers concurred that reporting internal team security concerns was a line (mid-level) manager responsibility. One explained: 'The monitoring aspects of what we do, risk indicators … it's in our expectations of line managers that they would have responsibility for understanding motivation and report to security if there is a change in that behaviour' (I19).

Similarly, several non-managers endorsed this perspective of line managers as central to team members' behavioural monitoring. Some appeared disengaged from any role in the organization's wider security culture, with

comments relating to colleagues not following the correct security procedures as 'not *my* problem' (I6). Accompanying such demarcation between non-managers and management roles was a sense of non-managers' powerlessness. Their position in the hierarchy evidently obfuscates their part in security: '[At] my lowly level, I probably don't have the understanding of an exec [utive]' (I15). Senior manager-led internal communication on all kinds of organizational matters appeared to specifically influence employees' lack of confidence concerning 'speaking up'. Direct experience of ineffective upwards communication and circulating stories about how such efforts have been received by management in the past created a climate at odds with the security culture. For example, one non-manager explained what happened when one, in their words, 'rocked the boat':

> You either just get ignored or 'oh god, he's off again' kind of mentality … there was one [employee] that blew the whistle on certain things and I personally think … he complained about the right thing to the wrong person and got hounded out (I15).

Vetting. A further concern, raised frequently by non-managers, that restrained their willingness to raise security concerns, involved the rigorous security vetting on which all employees' employment was conditional. In this organization, vetting involves ongoing disclosure of a wide range of personal information. The pivotal value of this security clearance to the ability to remain employed produced an unintended heightening of anxiety for employees in raising any potentially inappropriate concerns about colleagues. These fears spanned disclosure of mental health issues through to direct misconduct. As one non-manager reflected: 'There is always the concern that what you say will come back on you …. It's the whole thing of the [security] clearance' (I4). Anxiety, along with pride in their specialized expertise, was interwoven in employees' professional identities: 'We are working at a one-off place and there is an element of, "it's a privilege to have a specialised job… I wouldn't like to lose that' (I6). Paradoxically, as each employee is security-cleared, it arguably reduces their attention and vigilance towards others' behaviours. As one interviewee explained: 'It's not complacency, but there is a general feeling here that if you have been given one of these [security passes] you are trustworthy, we trust each other, and you do each other no harm' (I9). Inherent to professional security clearance were notions of professional ethics, denoting both employees' trustworthiness and implied discretion. Employees' 'special' identity might also produce a defensive silence (Van Dyne et al., 2003) towards others in this 'club'.

'Need to Know' Principle. A cornerstone of this shared professionalism is the 'need to know' principle. As a strong organization-wide value, it has

significant consequences for bottom-up communication, as well as lateral, peer-level communication. Interviewees across all participant groups concurred that they should not discuss, nor enquire, about aspects of work with which they were not directly involved; the high security nature of the organization's operations underpinned this ethos. However, a further unintended consequence was non-managers' reluctance to challenge their colleagues' behaviours, even when intuitively considered alarming, for fear of overstepping this cultural boundary. As one non-manager outlined:

> In terms of noticing behaviours and identifying issues within a team, they should be picked up by people … share and exchange, communicate more … sometimes this 'need to know' culture, where you blinker things off, gets to an extreme where people don't say anything. (I7)

Consequently, as both managers and non-managers reflected, this key principle fuelled their failures to engage with and discuss security breach incidents across the organization and restricted organizational learning opportunities. Such reluctance stemmed from a desire to protect the organization's reputation, as a senior manager explained:

> Lots of security incidents don't get talked about … partly because of the reputational risk to the organization, we don't want the press picking up [the information] … there is some support messaging needed to go out across the organization to say … here are some examples of how we have had to deal robustly with people, as a message to staff to make sure they remain compliant. (I19)

Senior managers thus recognized the value of sharing such information to enhance staff compliance; however, this connection between bottom-up compliance and top-down communication is problematic and comprises the focus of our next section.

Constraints to Top-Down Communication

Three significant factors were revealed in our analysis that constrained top-down security communication within this organization, diluting or fragmenting both shared understandings of inappropriate security behaviours and the organization's ability to mitigate actual insider threat incidents.

Balancing Formal and Informal Security Communication within a Strong Hierarchy. Traditionally, the organization had been heavily guided by written rules pertaining to procedures and employee behaviour, but the interviews revealed that management had attempted to introduce a less formal style of control:

> We have come from a place of being a very parent-child, rule compliant organization, with everything written down of expectations of staff … to a place of more trust and peer-peer relationships … it's all about giving some parameters for people to work in, but … taking grown up decisions for themselves. (I16)

However, both management and non-management responses reflected a relatively unchanged authoritarian organization with a persistent strong hierarchy, notably described as 'the treacle' (I17). While regarded by senior managers as a logical and protective structure, mid-level and non-managers viewed it and its accompanying bureaucracy as a barrier to clear communication, about security or otherwise: 'It [information] has to come down through several layers … I sometimes think that it doesn't come through with the same message' (I17). Although strategic changes to organizational communication culture were mirrored in shifts to more open physical workplaces, several interviewees commented that more support was needed in *how* to practically manage the transition to a new informal approach, especially pertaining to security reporting. A non-manager reflected:

> We are doing 'hot desking' [shared desk space] and everything like that … we are doing sharepoint … The only thing not open, which I think it should be, is that emotional, psychological bit—the part you say, 'that is missing from my colleague's understanding'. (I8)

Implicit Assumptions rather than Explicit Instruction. These transitions within the organization thus appeared to increase ambiguity for employees regarding how the 'need to know' principle should now be applied. Further, there was a lack of standardized employee guidance both on entering the organization and in navigating their working lives. A non-manager reflected the resultant consequences for the reported critical incident:

> It could well be that when [the SOI] 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. (I15)

Another mid-level manager concurred, outlining the necessity of clearer organizational communication and reinforcement around process controls: '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). There are particular consequences for security risk behaviours that do not fall within the standard threat parameters. As a mid-level manager explained: 'If it was a big pile of printed information … I would say shred it immediately. That's one of the warning signs [of insider threat] … [but] folder surfing was never a

warning sign that we were trained in' (I14). Indeed, this ambiguity is noted in the critical incident's disciplinary documentation with the SOI insisting that 'there had been comments made about their computer holdings, et cetera, but not a warning'. Indeed, neurodiversity can create subtle over-attention (Lorenz et al., 2016) causing the distinction between 'comments' versus 'a warning' to produce either an unwitting, or strategic, re-interpretation of managerial discourse that enables the gravity of actions to be diminished. It arguably also reflects a wider formal rule following organizational culture, rather than evidence of a deeper, reflexive engagement with complex notions of security.

Varying Managerial Approaches. Compounding organizational top-down security communication ambiguities further were evident differences in the local level approaches of managers. The regular restructuring of teams in response to an almost bi-annual transition at the top of the organization added further inconsistency. Preceding and during this critical incident, the SOI's team had multiple different managers, each sending varying signals as to what constituted acceptable security behaviours. One mid-level manager explained:

> We merged in with another group … suddenly you have got a different boss … and he is far less tolerant of sharing things [information], that's when it starts to trigger, ah yes, I need to warn people that you know, just having a folder full of information might not be acceptable. (I14)

Further consequences of leadership changes include the probability that individual warning signs go either unnoticed, or are insufficiently monitored by new incumbents who instead are focused on becoming acquainted with their new environment and relationships. Each leader transition produces fresh security uncertainty amongst non-managers with expectations and boundaries again shifting and autonomy levels being re-drawn; this leads to fragmentation within the security climate.

Discussion

Our research question asked, *what role, if any, does internal organizational communication play in insider threat behaviour?* Our findings indicate that internal organizational communication can, under certain conditions, play an enabling role in insider threat behaviour. Three communication flows are of particular significance, providing a simple but informative analytical strategy to examine how an organization's internal communication environment can unintentionally contribute to the emergence of insider threat: (1) top-down organizational communication from managers, (2) bottom-up communication from non-managers to managers and (3) lateral communication between peers.

Top-Down Communication

In our high security organization case study, top-down communication norms frame responsibility for insider threat-related reporting as a managerial preserve while discursively positioning non-managers as passive, in roles of compliance. Clear disconnects were evident between senior leaders' targeted attempts to transform security communication from a formal authoritarian, leader-follower approach into informal peer-to-peer based. Non-managers' consequent relative disengagement from security and silence positions only mid- and senior-level managers as 'in charge' of, and accountable for, reporting security concerns. Critically, peer–peer informal security monitoring becomes a vague organizational aspiration rather than an important security layer. Concurrent with these perceived role demarcations are tensions between senior- and mid-level managers regarding communication concerns. Mid-level managers align more often with non-manager perspectives, particularly concerning the barriers to effective security communication. This divergence within management levels exacerbates the fragmentation in climate regarding shared understandings and the enactment of security protocol.

Inconsistent managerial approaches to security were evident in this case. Leadership style and leadership communication have been widely discussed within the organizational literature, specifically how such factors have positive or negative impacts on employee security engagement and behaviour (e.g. Clarke, 2013; Willis et al., 2017). Our findings show how frequent team management changes compound these factors. Successive leaders with more active or passive approaches to internal security threats, as well as more or less openness and explicit discussions of security matters, have tangible consequences on employee perceptions and enactments of security. Frequent leadership changes directly contribute to divergent notions and manifestations of security within teams, including their proactive identification of threats, acknowledgement of their emergence, and willingness to speak up and to engage in their correction. Indeed, both managers and non-managers behave according to *their own* implicit assumptions and interpretations of 'security'. Our findings indicate a value to leaders dedicating time to understanding their role in the development and manifestations of security assumptions, notions of insider threat and the communicative framing of security climates across their organization. At a theoretical level, our findings are important to the development of more comprehensive models of crisis communication. They suggest that leaders help frame internal security communication – and therefore to some extent also resultant security behaviours – through both their explicit and unintentional communication. While SCCT, for instance, emphasizes how managers can promote certain interpretations of crisis to external stakeholders through a strategic communicative focus on certain issues and values (Coombs, 2007), our study reveals these framing effects arise, too,

from *unintentional* internal managerial communication. This advances our understanding of how this particular form of crisis, insider threat, can emerge in the first place.

Bottom-Up Communication

Our findings further suggest that bottom-up communication flow is significant in explaining the enabling role of internal communication in insider threat activity. We demonstrate how organizational communication norms, namely here the 'need to know' standard, can constrain bottom-up communication, effectively silencing individual employees from raising valid concerns about colleague behaviour to managers. This principle, together with formal security vetting, represents critical components of individuals' identities as trustworthy and discreet security professionals and illuminates the material significance of discursive outworkings of professional identity (Kornberger & Brown, 2007; Scott & Trethewey, 2008). Concurrently, the omission of clear and consensual understanding of the circumstances in which this principle should or should not be applied increases ambiguity about 'speaking up'. Distrust of the HR department – considered hostile by non-managers and unpredictable by managers – reinforces such hesitancy. Further, the distinct affective tone of fear of 'getting in trouble', reduces non-managers' (and in some cases mid-level managers') willingness to raise valid security concerns. Our findings here concur with prior research on the role of this emotion in silence (Kirrane et al., 2017) and of place in the hierarchy with the willingness to 'voice up' (e.g. see Morrison, 2014). Research on employee reticence to voice concerns explains how speaking up can challenge the powerful status quo, indicating a negative appraisal of current management practices, including detrimental repercussions for others, or simply as a futile activity from a lower-level employee (Morrison, 2014). In addition, the likely further consequences we reveal for mid-level managers in dealing with negative repercussions within their teams (e.g. staff disgruntlement, low morale), echo the selective silence that pervade from self-protection concerns. Direct experiences and vicarious learning on the viability of 'rocking the boat' produce self-protection needs (Sprague & Ruud, 1988), to create a form of 'taken for granted self-censorship' (Detert & Edmonson, 2011) in relation to authority figures.

Our findings support the curtailing of internal whistleblowing within organizations in which employees perceive themselves as having little organizational power compared to managers (Skivenes & Trygstad, 2010). Yet this form of employee voice is central to mitigating insider threat. Searle and Rice (2018) have dichotomized insider threat into active and passive forms, with passive threat constituted by the withdrawal behaviours of colleagues that serve to facilitate an insider's organizationally threatening activities. Similarly, Kassing's (2002) framework of employee voice distinguishes active-

passive from constructive-destructive dimensions, to conceptualize upward communication (voice) as a form of dissent. The type of voice we detect in this case aligns with passive-destructive voice, which is characterized by 'murmurings, apathy, calculated silence, and withdrawal' (Kassing, 2002, p.191), and with acquiescent silence (Van Dyne et al., 2003). Further, within a wider organizational culture that comprises little active dissent towards authority, we also see prosocial silence – derived from a team protection motive – and defensive silence, which serves as a means of maintaining their security clearance and professional identities. These distinct drivers and forms of silence – acquiescent, defensive and prosocial (Van Dyne et al., 2003) – constitute warning signs of potential insider threat activity.

Lateral Communication

Our findings thus far represent an imbalance in power relations between managers and non-managers in this organization, but they also illuminate the significant influence of individuals and groups without formal leadership roles in sensemaking around organizational security. We demonstrate the criticality of local team dynamics and social roles in the development of communication norms that legitimize risky behaviour and produce forms of collective moral disengagement (Bandura, 2016). 'Nerds', 'geeks' and 'on the spectrum' were terms interviewees repeatedly used to discuss themselves and others in this organization, providing the potential to excuse counterproductive work identities and norms of behaviour (c.f. Creech, 2020). Further, we found growing employee and management recognition that neurodiversity diagnosis and support could be invaluable for some employees. The critical incident case does include an individual who was subsequently diagnosed as having Autism Spectrum Disorder (ASD); our study therefore, reflects how insider threat behaviours can involve a complex interplay of environmental and individual difference factors. Individuals on the autistic spectrum may be overrepresented in particular sectors, notably science and technology (Baron-Cohen et al., 2001). These individuals possess a host of positive qualities (e.g. attention to detail, pattern recognition), concurrent with occasional requirement for further workplace support to better navigate communication and social challenges (Lorenz, et al., 2016). Digital hoarding behaviour *may* be associated with ASD (Van Bennekom et al., 2015), but it is also common within general working populations and is increasingly recognized as a security risk in modern organizations (Neave et al., 2020). Importantly, research indicates good practice towards neurotypical individuals in the workplace *is* good practice (Hagner & Cooney, 2005).

A further lateral communication dimension in this critical incident is the strength of team cohesion and an arguably misplaced local loyalty (Hildreth & Anderson, 2018). Yet this case arose partly in response to the replacement of

HR procedures considered important by this team (promotion). The opacity of the new requirements prompted the SOI to fill the resultant information void; thus, it was a direct response to inadequate organizational communication. An additional facet of this team's cohesion that contributed to the insider threat was the use of humour and its unintended consequences. Extant research shows humour has a number of important social functions, several of which apply to this case (Wood & Niedenthal, 2018). First, humour offers a means of rewarding and reinforcing individuals' behaviour, here tacitly encouraging and inadvertently condoning the SOI's activities. Second, it can ease social tension and signal team affiliation through teasing and banter. Third, it produces non-confrontational reinforcement of social rules, here team citizenship, at the expense of organizational rule compliance. Further, within cognitively diverse teams, humour's subtler messaging for these latter two functions may not be acknowledged by those with ASD due to important neurological cognitive and affective processing differences (Lyons & Fitzgerald, 2004). Critically, laughter can offer an important coping mechanism alleviating embarrassment and managing anxiety that can arise from moral threats, creating both a way to disengage and diminish the significance of these organizationally threatening actions (Page & Pina, 2015). Our critical incident team members registered the subtle corrective messaging of their ironic humour serving multiple functions, deflecting serious risk, reframing the SOI's actions as benign and preserving both team and professional credibility (Kwon et al., 2020; McCreaddie & Harrison, 2018) without having to directly face its potentially negative security implications. Our findings support the significant role of humour, social influence and local loyalty (Desmond & Wilson, 2018) in reducing individuals' internal whistleblowing, especially where risky behaviour is regarded as well intentioned (Hildreth & Anderson, 2018). In this context, selective silence is pro-social (Van Dyne et al., 2003) as well as personally beneficial (Stouten et al., 2019).

Conclusions

This study has revealed the enabling and unintentional role of internal organizational communication in one under-researched form of organizational crisis, insider threat. In doing so, we make three important research contributions to the areas of organizational communication, organizational crisis, security and insider threat, which have practical value for organizational managers.

First, we demonstrate that insider threat can, and should, be considered a form of potential organizational crisis in which internal organizational communication may play an enabling role. Communication frames matter, not just for strategic external communication with stakeholders in the aftermath of a crisis, but also to enhance understanding of how crisis emerges in the first

place through employees' accrual of intended and unintended security messages. Second, we advance insight into the fragmentation of security climates that create barriers to bottom-up communication and employee voice and result in selective collective silence around insider threat activity. Bottom-up selective silence represents, on the one hand, loyalty and empathy for particular local relationships, with individuals' problematic work behaviours reframed as benign; and on the other, reticence to raise valid concerns to organizational authorities and senior managers because of fear of their perceived over-reaction to minor non-malicious misdemeanours. Employee selective silence is symptomatic of a closed-communication environment, characterized by hierarchies, technical rules and formal reporting of concerns regarded essentially as a manager's role. High stakes vetting may facilitate both a belief that trustworthy individuals are employed in a workplace and that individuals operate within a 'safe harbour' (Bienefeld & Grote, 2014). Conversely, in such an environment, problematic or unsafe behaviours may flourish undetected. Accordingly, when internal whistleblowing fundamentally conflicts with one's team norms and professional identity (in this case, being discreet), reporting will be reduced (e.g. Gravley et al., 2015). Our findings therefore strengthen the value of challenging leader-centric perspectives on power in organizations to instead consider the interplay and coherence between different organizational levels and employee perceptions (Dannals et al., 2020; Fairhurst & Connaughton, 2014) in enhancing effective and secure functioning.

Third, we demonstrate that the skewed balance away from 'softer' elements of security communication, specifically role clarity and relational and behavioural expectations, in favour of formal elements including vetting, policies and discipline can be detrimental to all three internal communication flows. Rebalancing in this respect might be of particular value to science and technology organizations, which are more likely to employ greater numbers of neurodiverse individuals who may particularly struggle in contexts with inconsistent and intangible directives and social cues (Baron-Cohen et al., 2001).

Limitations and Further Research

As is common to qualitative interview-based research, our data comprises personal and retrospective recall derived from a sample of interviewees (largely from a similar demographic) within one relatively unique organization. Future research might investigate the generalizability of our findings, both within and beyond high security organizations. Individuals from different organizations, with different professional identities and work norms (which do not prioritize hierarchical authority, confidentiality and discretion), might provide quite different results. Nonetheless, we propose that our three-flow communication framework can be usefully applied elsewhere.

Additionally, we encountered a variety of issues associated with case study research, such as the fact that the critical incidents examined were framed as such by senior managers in the organization. There is no doubt that the need for access influenced the research process (Riese, 2019). However, through a process of relationship building and a genuine spirit of academic–practitioner collaboration on a common objective (understanding the protective security of organizations), we were able to cultivate a space for constructive and critical engagement that we hope is evident in this paper and worthwhile to our academic and practitioner colleagues alike.

Appendix A

Interviewee 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

Acknowledgements

We wish to thank the anonymous reviewers of our paper for their thoughtful and supportive feedback. We also gratefully acknowledge the participation of our case study organization and interviewees who provided such rich insights. Lastly, we thank *the Centre for Research and Evidence on Security Threats (CREST)* who funded this research [ESRC Award: ES/N009614/1].

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was funded by the Centre for Research and Evidence on Security Threats (ESRC Award: ES/N009614/1), which is funded in part by the UK security and intelligence agencies (see the public grant decision here: https://gtr.ukri.org/projects?ref=ES%2FV002775%2F1). The funding arrangements required this paper to be reviewed to ensure that its contents did not violate the Official Secrets Act nor disclose sensitive, classified and/or personal information.

ORCID iD

Charis Rice https://orcid.org/0000-0003-2094-4597

Notes

1. https://www.cpni.gov.uk/critical-national-infrastructure-0.
2. One individual was interviewed via telephone due to their availability.
3. One individual was interviewed twice due to their role as an insider threat specialist who provided: (1) an overview of all selected insider threat cases, associated official handling procedures by management and important security context information; (2) a personal perspective on the development of the insider threat cases and the organization's general and security-specific culture.

References

Bandura, A (2016). *Moral disengagement: How people do harm and live with themselves*. Worth Publishers.

Baron-Cohen, S., Wheelwright, S., Skinner, R., Martin, J., & Clubley, E. (2001). The autism-spectrum quotient (AQ): Evidence from asperger syndrome/high-functioning autism, males and females, scientists and mathematicians. *Journal of Autism and Developmental Disorders*, *31*(1), 5–17. https://doi.org/10.1023/A:1005653411471.

Bienefeld, N., & Grote, G. (2014). Speaking up in ad hoc multiteam systems: Individual-level effects of psychological safety, status, and leadership within and across teams. *European Journal of Work and Organizational Psychology*, *23*(6), 930–945. https://doi.org/10.1080/1359432X.2013.808398.

Bisel, R. S., & Adame, E. A. (2018). Encouraging upward ethical dissent in organizations: The role of deference to embodied expertise. *Management Communication Quarterly*, *33*(2), 139–159. https://doi.org/10.1177/0893318918811949.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Braun, V., & Clarke, V. (2020). 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., Colville, I., & Pye, A. (2015). Making sense of sensemaking in organization studies. *Organization Studies*, *36*(2), 265–277. https://doi.org/10.1177/0170840614559259.

Brown, A. D., & Coupland, C. (2015). Identity threats, identity work and elite professionals. *Organization Studies*, *36*(10), 1315–1336. https://doi.org/10.1177%2F0170840615593594.

Clarke, S. (2013). Safety leadership: A meta-analytic review of transformational and transactional leadership styles as antecedents of safety behaviours. *Journal of Occupational and Organizational Psychology*, *86*(1), 22–49. https://doi.org/10.1111/j.2044-8325.2012.02064.x.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, *10*(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049.

Creech, G. E. (2020). "Real" insider threat: Toxic workplace behavior in the intelligence community. *International Journal of Intelligence and CounterIntelligence*, *33*(4), 682–708. https://doi.org/10.1080/08850607.2020.1789934.

Dannals, J. E., Reit, E. S., & Miller, D. T. (2020). From whom do we learn group norms? Low-ranking group members are perceived as the best sources. *Organizational Behavior and Human Decision Processes*, *161*(2020), 213–227. https://psycnet.apa.org/doi/10.1016/j.obhdp.2020.08.002.

Denner, N., Viererbl, B., & Koch, T (2019). A matter for the boss? How personalized communication affects recipients' perceptions of an organization during a crisis. *International Journal of Communication*, *13*, 2026–2044. https://ijoc.org/index.php/ijoc/article/view/10791.

Desmond, J., & Wilson, F. (2018). Democracy and worker representation in the management of change: Lessons from Kurt Lewin and the Harwood studies. *Human Relations*, *72*(11), 1805–1830. https://doi.org/10.1177/0018726718812168.

Detert, J. R., Burris, E. R., Harrison, D. A., & Martin, S. R. (2013). Voice flows to and around leaders. *Administrative Science Quarterly*, *58*(4), 624–668. https://doi.org/10.1177/0001839213510151.

Detert, J. R., & Edmondson, A. C. (2011). Implicit voice theories: Taken-for-granted rules of self-censorship at work. *Academy of Management Journal*, *54*(3), 461–488. https://doi.org/10.5465/AMJ.2011.61967925.

D'Urso, S. C (2006). Who's watching us at work? Toward a structural–perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*, *16*(3), 281–303. https://doi.org/10.1111/j.1468-2885.2006.00271.x.

Dyne, L. V., Ang, S., & Botero, I. C. (2003). Conceptualizing employee silence and employee voice as multidimensional constructs*. *Journal of Management Studies*, *40*(6), 1359–1392. https://doi.org/10.1111/1467-6486.00384.

Edmonson, A (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, *44*(2), 350–383. https://doi.org/10.2307/2666999.

Eglene, O., Dawes, S. S., & Schneider, C. A. (2007). Authority and leadership patterns in public sector knowledge networks. *The American Review of Public Administration*, *37*(1), 91–113. https://doi.org/10.1177/0275074006290799.

Fairhurst, G. T., & Connaughton, S. L. (2014). Leadership: A communicative perspective. *Leadership*, *10*(1), 7–35. https://doi.org/10.1177/1742715013509396.

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

Ford, J. L., & Stephens, K. K. (2018). Pairing organizational and individual factors to improve employees' risk responsiveness. *Management Communication Quarterly*, *32*(4), 504–533. https://doi.org/10.1177%2F0893318918774418.

Gravley, D., Richardson, B. K., & Allison, J. M. (2015). Navigating the "Abyss". *Management Communication Quarterly*, *29*(2), 171–197. https://doi.org/10.1177/0893318914567666.

Hagner, D., & Cooney, B. F. (2005). "I do that for everybody": Supervising employees with autism. *Focus on Autism and Other Developmental Disabilities*, *20*(2), 91–97. https://doi.org/10.1177/10883576050200020501.

Hildreth, J. A. D., & Anderson, C. (2018). Does loyalty trump honesty? Moral judgments of loyalty-driven deceit. *Journal of Experimental Social Psychology*, *79*(2018), 87–94. https://doi.org/10.1016/j.jesp.2018.06.001.

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.

Kassing, J. W. (2002). Speaking up. *Management Communication Quarterly*, *16*(2), 187–209. https://doi.org/10.1177%2F089331802237234.

Kim, Y. (2018). Enhancing employee communication behaviors for sensemaking and sensegiving in crisis situations. *Journal of Communication Management*, *22*(4), 451–475. https://doi.org/10.1108/JCOM-03-2018-0025.

Kim, Y., Kang, M., Lee, E., & Yang, S-U (2019). Exploring crisis communication in the internal context of an organization: Examining moderated and mediated effects of employee-organization relationships on crisis outcomes. *Public Relations Review*, *45*(3), 101177. https://doi.org/10.1016/j.pubrev.2019.04.010.

Kirrane, M., O'Shea, D., Buckley, F., Grazi, A., & Prout, J. (2017). Investigating the role of discrete emotions in silence versus speaking up. *Journal of Occupational and Organizational Psychology*, *90*(3), 354–378. https://doi.org/10.1111/joop.12175.

Knight, R., & Nurse, J (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*(2020), 1–18. https://doi.org/10.1016/j.cose.2020.102036.

Kornberger, M., & Brown, A. D. (2007). Ethics' as a discursive resource for identity work. *Human Relations*, *60*(3), 497–518. https://doi.org/10.1177/0018726707076692.

Kwon, W., Mackay, R., Clarke, I., Wodak, R., & Vaara, E. (2020). Testing, stretching, and aligning: Using 'ironic personae' to make sense of complicated issues. *Journal of Pragmatics*, *166*(2020), 44–58. https://doi.org/10.1016/j.pragma.2020.06.001.

Larkin, M., Watts, S., & Clifton, E. (2006). Giving voice and making sense in interpretative phenomenological analysis. *Qualitative Research in Psychology*, *3*(2), 102–120. https://doi.org/10.1191/1478088706qp062oa.

Legg, P., Moffat, N., Nurse, J.R.C., & Happa, J (2013). Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *4*(4), 20–37. https://doi.org/10.22667/JOWUA.2013.12.31.020.

Lewis, L. K., Hamel, S. A., & Richardson, B. K. (2001). Communicating change to nonprofit stakeholders. *Management Communication Quarterly*, *15*(1), 5–41. https://doi.org/10.1177/0893318901151001.

López-Couso, M. J., & Méndez-Naya, B. (2012). On the use of as if, as though, and like in present-day English complementation structures. *Journal of English Linguistics*, *40*(2), 172–195. https://doi.org/10.1177/0075424211418976.

Lorenz, T., Frischling, C., Cuadros, R., & Heinitz, K. (2016). Autism and overcoming job barriers: Comparing job-related barriers and possible solutions in and outside of autism-specific employment. *Plos One*, *11*(1), e0147040. https://doi.org/10.1371/journal.pone.0147040.

Lyons, V., & Fitzgerald, M. (2004). Humor in autism and asperger syndrome. *Journal of Autism and Developmental Disorders*, *34*(5), 521–531. https://doi.org/10.1007/s10803-004-2547-8.

Mao, C. M., & DeAndrea, D. C. (2018). How anonymity and visibility affordances influence employees' decisions about voicing workplace concerns. *Management Communication Quarterly*, *33*(2), 160–188. https://doi.org/10.1177/0893318918813202.

McCreaddie, M., & Harrison, J. (2018). Humour and laughter. In O Hargie (Ed.), *The handbook of communication skills* (4th ed., pp. 287–317). Routledge.

Men, L. R. (2014). Strategic internal communication. *Management Communication Quarterly*, *28*(2), 264–284. https://doi.org/10.1177/0893318914524536.

Men, R. L., & Bowen, S.A (2017). *Excellence in internal communication management*. Business Expert Press.

Morrison, E. W. (2014). Employee voice and silence. *Annual Review of Organizational Psychology and Organizational Behavior*, *1*(1), 173–197. https://doi.org/10.1146/annurev-orgpsych-031413-091328.

Neave, N., Briggs, P., Silence, E., & McKellar, K (2020). *Cybersecurity risks of digital hoarding behaviours*. CREST. https://crestresearch.ac.uk/resources/cybersecurity-risks-of-digital-hoarding-behaviours/.

Nerstad, C. G. L., Searle, R., Černe, M., Dysvik, A., Škerlavaj, M., & Scherer, R. (2017). Perceived mastery climate, felt trust, and knowledge sharing. *Journal of Organizational Behavior*, *39*(4), 429–447. https://doi.org/10.1002/job.2241.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M (2014). Understanding insider threat: A framework for characterising attacks. In IEEE Security and Privacy Workshops (SPW), San Jose, CA, 17–18 May, 2014. (pp. 214–228). IEEE. https://doi.org/10.1109/SPW.2014.38.

Page, T. E., & Pina, A. (2015). Moral disengagement as a self-regulatory process in sexual harassment perpetration at work: A preliminary conceptualization. *Aggression and Violent Behavior*, *21*, 73–84. https://doi.org/10.1016/j.avb.2015.01.004.

Patton, M. Q (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed). Sage.

Payne, G., & Payne, J (2004). *Key concepts in social research*. Sage. https://www.doi.org/10.4135/9781849209397.

Riese, J. (2019). What is 'access' in the context of qualitative research? *Qualitative Research*, *19*(6), 669–684. https://doi.org/10.1177/1468794118787713.

Robinson, S. L., Wang, W., & Kiewitz, C. (2014). Coworkers behaving badly: The impact of coworker deviant behavior upon individual employees. *Annual Review of Organizational Psychology and Organizational Behavior*, *1*(1), 123–143. https://doi.org/10.1146/annurev-orgpsych-031413-091225.

Schneider, B., Ehrhart, M. G., & Macey, W. H. (2013). Organizational climate and culture. *Annual Review of Psychology*, *64*, 361–388. https://doi.org/10.1146/annurev-psych-113011-143809.

Scott, C. W., & Trethewey, A. (2008). Organizational discourse and the appraisal of occupational hazards: Interpretive repertoires, heedful interrelating, and identity at work. *Journal of Applied Communication Research*, *36*(3), 298–317. https://doi.org/10.1080/00909880802172137.

Searle, R. H. (2018). Trust and HRM. In R. H. Searle, A.M. Nienaber, & S. Sitkin (Eds.), *Routledge companion to trust* (pp. 483–505). Routledge.

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

Searle, R. H., Rice, C., McConnell, A., & Dawson, J (2017). *Bad apples? Bad barrels? Or bad cellars? Antecedents and processes of professional misconduct in UK health and social care: Insights into sexual misconduct and dishonesty*. Professional Standards Authority. https://www.professionalstandards.org.uk/docs/default-source/publications/research-paper/antecedents-and-processes-of-professional-misconduct-in-uk-health-and-social-care.pdf.

Seeger, M. W., & Ulmer, R. R. (2003). Explaining Enron. *Management Communication Quarterly*, *17*(1), 58–84. https://doi.org/10.1177%2F0893318903253436.

Sellnow, T. L, & Seeger, M. W (2013). *Theorizing crisis communication*. John Wiley & Sons.

Shaw, E. D., Ruby, K. G., & Post, J. M (1998). The insider threat to information systems. *Security Awareness Bulletin*, *2–98*(1998), 27–47.

Skivenes, M., & Trygstad, S. C. (2010). When whistle-blowing works: The Norwegian case. *Human Relations*, *63*(7), 1071–1097. https://doi.org/10.1177/0018726709353954.

Sprague, J., & Ruud, G. L. (1988). Boat-rocking in the high-technology culture. *American Behavioral Scientist*, *32*(2), 169–193. https://doi.org/10.1177/0002764288032002009.

Stake, R. E (1995). *The art of case study research*. Sage.

Stouten, J., Tripp, T.M., Bies, R.J., & De Cremer, D (2019). When something is not right: The value of silence. *Academy of Management Perspectives*, *33*(3), 323–333.

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

B. C. Taylor, & H. Bean (Eds.), (2019). *The handbook of communication and security*. Routledge.

Van Bennekom, M. J., Blom, R. M., Vulink, N., & Denys, D (2015). A case of digital hoarding. *Bmj: British Medical Journal*. Case Rep. 2015, Oct 8 https://doi.org/10.1136/bcr-2015-210814.

Walden, J. A., & Kingsley Westerman, C. Y. (2018). Strengthening the tie: Creating exchange relationships that encourage employee advocacy as an organizational citizenship behavior. *Management Communication Quarterly*, *32*(4), 593–611. https://doi.org/10.1177/0893318918783612.

Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validity in qualitative research. *Qualitative Health Research*, *11*(4), 522–537. https://doi.org/10.1177/104973201129119299.

Whitty, M. (2021). Developing a conceptual model for insider threat. *Journal of Management & Organization*, *27*(5), 911–929. https://doi.org/10.1017/jmo.2018.57.

Wieland, S. M. B. (2020). Constituting resilience at work: Maintaining dialectics and cultivating dignity throughout a worksite closure. *Management Communication Quarterly*, *34*(4), 463–494. https://doi.org/10.1177/0893318920949314.

Willis, S., Clarke, S., & O'Connor, E. (2017). Contextualizing leadership: Transformational leadership and management-by-exception-active in safety-critical contexts. *Journal of Occupational and Organizational Psychology*, *90*(3), 281–305. https://doi.org/10.1111/joop.12172.

Wood, A., & Niedenthal, P (2018). Developing a social functional account of laughter. *Social and Personality Psychology Compass*, *12*(4), 1–14. e12383 https://doi.org/10.1111/spc3.12383.

Author Biographies

Charis Rice, PhD, is Assistant Professor at the Centre for Trust, Peace and Social Relations, Coventry University, the UK. Her main research interests include the communication of security, counterproductive work behaviour, strategic communication and trust.

Rosalind H. Searle, PhD, holds the Chair of Human Resource Management (HRM) and Organisational Psychology at the Adam Smith Business School, University of Glasgow, UK. She is Director of the European Association of Work and Organisational Psychology's (EAWOP) Impact Incubator. Her main research interests include counterproductive work behaviour, decent work, and HRM and trust in organizations.