Human Factors

Sorting Insiders from Co-workers: Remote synchronous computer-mediated triage for investigating insider attacks

Journal:	*Human Factors : The Journal of the Human Factors and Ergonomics Society*
Manuscript ID	HF-21-7387.R2
Manuscript Type:	Research Article
Keywords:	Risk assessment < ACCIDENTS, HUMAN ERROR, Human-automation interaction < AUTOMATION, EXPERT SYSTEMS, Automatic and controlled processing < COGNITION, Dual task, time sharing, task switching < COGNITION, Language < COGNITION, Mental workload < COGNITION, Situated cognition < COGNITION

Sorting Insiders from Co-workers: Remote synchronous computer-mediated triage for investigating insider attacks

Coral J. Dando [1], Paul J. Taylor [2], Thomas C. Ormerod [3], Linden J. Ball [4], Alexandra L. Sandham [5], Tarek Menacere [2]

[1] Dept. of Psychology, University of Westminster, London

[2] Dept. of Psychology, Lancaster University

[3] School of Psychology, University of Sussex

[4] School of Psychology, University of Central Lancashire

[5] Dept. of Psychology, University of Gloucestershire

Acknowledgments: This research was funded by the UK Gov, Project Ref. LUR 46.851.

Correspondence should be addressed to:

Coral J. Dando,
Dept of Psychology,
University of Westminster, London.
Email: c.dando@westminster.ac.uk

Research Article

Key words: Insiders; Computer-mediated triage; Deception; Investigation

The data that support the findings of this study are available from the corresponding author upon reasonable request.

WORD COUNT: 4497 (excludes structured abstract, precis, bios, title page contents, key points, text in tables, figures and references)

Abstract

Objective: Develop and investigate the potential of a remote, computer mediated and synchronous text-based triage, which we refer to as *InSort,* for quickly highlighting persons of interest after an insider attack.

Background: Insiders maliciously exploit legitimate access to impair the confidentiality and integrity of organizations. The globalisation of organisations and advancement of information technology means employees are often dispersed across national and international sites, working around the clock, often remotely. Hence, investigating insider attacks is challenging. However, the cognitive demands associated with masking insider activity offer opportunities. Drawing on cognitive approaches to deception and understanding of deception-conveying features in textual responses we developed InSort, a remote computer mediated triage.

Method: During a 6-hour immersive simulation, participants worked in teams, examining password protected, security sensitive databases and exchanging information during an organized crime investigation. Twenty-five percent were covertly incentivized to act as an 'insider' by providing information to a provocateur.

Results: Responses to InSort questioning revealed insiders took longer to answer investigation relevant questions, provided impoverished responses, and their answers were less consistent with known evidence about their behaviors than co-workers.

Conclusion: Findings demonstrate InSort has potential to expedite information gathering and investigative processes following an insider attack.

Application: InSort is appropriate for application by non-specialist investigators and can be quickly altered as a function of both environment and event. InSort offers a clearly defined, well specified, approach for use across insider incidents, and highlights the potential of technology for supporting complex time critical investigations.

Precis

Insiders exploit legitimate access to negatively affect organizations. Drawing on cognitive approaches to deception and understanding of deception-conveying features in textual responses we combined these literatures to develop ‘InSort’, a novel, remote computer-mediated triage. Findings suggest InSort has potential to triage persons of interest from co-workers following an attack, thereby expediting the initial investigative process.

Introduction

Insiders exploit privileged access to damage organizations (see Mills et al., 2017; Posey et al., 2013). Examples include a BUPA employee who downloaded and offered for sale 547,000 items of patient information and a NASA employee who downloaded classified national defence information. Insider crime is increasing (Homoliak et al., 2019; Clearswift Insider Threat Index, 2017) and becoming more expensive (European Union Agency for Cybersecurity, 2020; National Law Review, 2020). Surveys suggest 27% of cybercrime incidents are committed by insiders (Trzeciak, 2019) with insiders responsible for 43% of data loss reported by the world's largest companies (Intel Security, 2015). Insider threats are difficult to mitigate. Employees are trusted, with detailed knowledge and access to employer assets. Understanding of insider behaviours and psychological characteristics is improving (e.g., Costa, et al., 2016; Elmrabit et al., 2020; Greitzer et al., 2018; Spitzner, 2003; Taylor et al., 2013). However, few insider investigative techniques exist (Maybury, 2006) because knowledge derived from one attack is not necessarily relevant to others (e.g., CPNI, 2020; Saxena et al., 2020).

Computer-Mediated Triage

Gathering post attack information is fundamental to understanding what has happened. In doing so, investigators (in-house security or external agencies) seek to understand the veracity of employee accounts. Employees may be dispersed across numerous national or international sites and so conducting timely and effective investigations can be challenging. Here, we evaluate text-based computer mediated communication (CMC) using a series of event-specific questions towards meeting this challenge. CMC screening is increasingly used to support decision-making where there are high volumes of traffic such as for pre-screening job applicants and completing employee credibility assessments (Jenson et al., 2010; Tyman et al., 2014). Building on research concerning the language of insiders

(Jenkins & Dando, 2011; Taylor et al., 2013), we investigated whether synchronous textual responses to CMC questions might effectively triage persons of interest.

CMC has several potential advantages. Organizations can gather information from employees simultaneously, irrespective of location, offering speed, volume, and reach (e.g., Lew et al., 2018; Pang et al., 2018; Yao & Ling, 2020). Text-based CMC is widely accessible, technically stable and is low in media richness and so devoid of non-verbal cues that occur during face-to-face interactions that can negatively impact investigations, potentially reducing false positives and negatives (e.g., Bond & DePaulo, 2006; Dando & Ormerod, 2017; Is baster & Nass, 2000; Markowitz , 2020; Matsumoto et al., 2011; Meissner & Lyles, 2019; Nortje & Tredoux, 2019; ; Walsh et al., 2018).

Masking Malicious Behaviour

Psychological knowledge of the challenges of masking malicious activity offers strategic insight into how to structure a CMC triage. To remain above suspicion necessitates deceiving colleagues (e.g., Homoliak et al, 2019; Lew et al., 2018; Taylor et al., 2013). Hence, insiders have an impression management goal (Colwell et al., 2006; Weiss et al., 2006). They have to provide deceptive accounts that appear truthful and so have to manage 'two employment worlds': tasks they should and should not have completed. Hence, providing a convincing false account is more demanding than completing legitimate activity and then providing a truthful account. This disparity offers opportunities for detection (e.g., Colwell et al., 2007; Kohan et al., 2020; Vrij et al., 2017).

Increased cognitive load in such circumstances (e.g., Bhatt et al., 2009; Jiang et al., 2015) can result in differential verbal behaviours between liars and truthtellers. Liars often provide less consistent or coherent verbal accounts lacking informational content, with fewer event details (Boggard et al., 2016; DePaulo et al., 2003; Hartwig et al. 2011). Differences can be enhanced by tactical questioning techniques (e.g., Blandon-Gitlin et al., 2014; Dando

& Bull, 2011; Dando & Ormerod, 2020; Hamlin et al., 2020; Ormerod & Dando, 2015; Sporer, 2016; Vrij et al., 2010), which have yielded over 70% accuracy where the base rate of deceivers was just 1:1000 (Dando & Ormerod, 2020; Ormerod & Dando, 2015), compared with a typical detection rate of 54% (e.g., Bond & dePaulo, 2006; Hauch et al., 2016). Similar results are reported in laboratory-based research (e.g., Dando & Bull, 2011; Granhag & Hartwig, 2015; Levine, 2014; Sandham et al., 2020).

Detecting deception via tactical questioning is largely situated in face-to-face and media-rich interview contexts. Nonetheless, several techniques lend themselves to CMC triage with potential for leveraging measurable indicators of deception (Lee et al., 2009; Zhou et al., 2002), particularly where comparisons can be made across employee responses gathered following each insider attack (Burgoon et al., 2003; Rubin et al., 2015). For example, deception-conveying features can sometimes include wordy replies with low information (e.g., Pollina et al., 2017; Vendemia et al., 2005) and more expressions of uncertainty (Zhou et al., 2002).

Towards a Solution

Combining cognitive approaches to deception and understanding of deception-conveying features in textual responses, we developed a novel CMC text-based triage: *InSort* (**In**sider **Sort**). InSort comprised a series of bespoke questions dictated by the insider event itself, the run-up to the event, and workers day-to-day work activities (e.g., necessary, unnecessary, and not allowed). Additionally, various questioning strategies were employed. Target questions concern attack-specific behaviours, including behaviours in the run up to an attack, questions about attempted access to databases, physical movements, and communication. Target questioning increases cognitive complexity for insiders to maximize the collection of triage-relevant information. Open questions (tell, explain, describe) gather accounts about specific times, necessitating provision of expansive answers. These question types and their tactical presentation makes it challenging for insiders to provide a coherent account (e.g., Dando & Ormerod, 2020; Dando & Bull 2011; Ormerod & Dando, 2015).

Target questions are manipulated to impose high cognitive demands on liars. They are not presented *en bloc* nor chronologically, thereby introducing a temporal element (requiring maintenance of six worlds – true and false versions of past, present and future). Some target questions are repeated, accentuating between-question inconsistencies and contradictions, which can be indicative of deceit (Blair et al., 2018; Chan & Bull, 2014; Vredeveldt et al. 2014). Responses are required before moving to the next question. Thus, InSort is interactive (e.g., Lee et al., 2009; Sánchez-Junquera et al., 2020; Zhou et al., 2003), demanding higher levels of cognitive engagement (Burgoon et al., 2010). The immediacy of InSort reduces opportunities to construct deceptive accounts or confer with accomplices versus lengthier triage processes conducted by human investigators (Levine & Blair, 2018; Walczyk et al., 2013).

In sum, InSort may confer advantages including speed of implementation and increased concurrent cognitive demand for insiders (deceivers), which may leverage deception-conveying features (e.g., Bhatt et al., 2009; Jiang et al., 2015). We conducted a 'serious gaming' empirical study, whereby participants were immersed in a full-day office-based collaborative investigations of organized crime. The game, known as Confidential Operations Simulation (iCOS: see Taylor et al., 2013), was played over a series of competitive rounds. To establish a behavioural baseline, the first round was played with no insider. In subsequent rounds, team members were assigned the role of 'insider', receiving financial incentives to undertake illicit activities and not to be caught (see Method). The study tested a series of hypotheses:

- Insiders will take significantly longer than non-insiders to complete InSort (H^1) because of the dual impacts of tactical questioning and limited time to develop lie scripts.

- Impression management will result in insider's text responses to open target questions being shorter and with less information than non-insiders (H^2).
- Insiders will be less consistent in their responses to closed target questions , making answer-evidence errors (H^3).
- Insiders will report finding InSort cognitively demanding and will be less confident in their responses (H^4).

Method

Participants and Procedure

Sixty participants were paid £50 to take part in iCOS games lasting between 6 and 9 hours (*M* = 6.8 hours) - 26 males (M_{age} = 25.67, range 18 to 40 years), and 34 females (M_{age} = 23.8 years, range 19 to 30 years). Each game was split into four rounds and comprised 12 players, randomly assigned to a team (i) Fraud; (ii) Human Trafficking; and (iii) Narcotics. Each team comprised four roles: Administrator, Field Agent, Intelligence Analyst and Tactical Investigator. Status and responsibilities within teams were equal.

Teams had to solve a series of linked crimes, one in each round. Teams were presented with intelligence updates about criminal gangs and used this information to guide their searches of password-protected databases. Team players pieced together information to identify gang members and their location. Players' database access was limited, so team members worked together, exchanging information, recognizing connections across databases, and engaging in collaborative problem solving. The team that most quickly identified and located criminals 'won'. Teams were financially incentivized to win each round (an additional £20 for winning the round). Each round lasted approximately ninety minutes including regular breaks.

At the start, participants were randomly assigned to a team role. They received instructions about the tasks to be completed, training on using the investigative databases, and familiarized themselves with the databases. To simulate a secure environment, players worked in 'silent' offices, making notes using desktop publishing and spreadsheet software and exchanging information using email, SMS messaging and mobile phone conversations. They had access to a printer in a separate room. Once familiar with the environment, one team member received instructions about the first crime to be investigated. All further interaction with participants was conducted via email with 'Gold Command' (a confederate). Gold Command issued instructions for subsequent tasks. By embedding task instructions into the simulation, we hoped to enhance participants' immersion in the simulation (Druckman, 2005).

Prior to the second round (at the end of the first round), up to two players in each team were covertly approached to provide information to a provocateur for an additional £20 reward. Specifically, to obtain information concerning an individual under investigation, and to email this information to the provocateur. The approach occurred face-to-face, out of sight of the other participants. The same participants were again covertly invited to complete further acts in the third and fourth rounds for an additional £20 each time. They were instructed to develop their own method for completing the insider task to avoid raising suspicion of teammates. All participants approached agreed to the insider task. The multiple teams and sequence of rounds provided insiders numerous opportunities to complete their tasks. For example, they could develop friendships with members of other teams for malicious information gathering or distribute their activity across multiple periods to make it more difficult to spot patterns of activity. Similarly, breaks taken by co-workers afforded opportunities for players to compromise security.

Investigative tasks increased in complexity throughout the game. Similarly, the insider task increased in complexity. In round 2, insiders were instructed to retrieve information from a database they had legitimate access to but which was irrelevant to their team's intelligence task. In round 3, to provide information from a database only legitimately accessible by another team member. In round 4, to gather information from a database that was only accessible by members of another team. Once the game was complete, players were informed that there had been a security breech, and that their behaviour during the simulation would investigated. Each participant was then required to individually complete InSort. All insiders completed each of the insider tasks set.

Materials

The iCOS software comprised five primary modules: a password-protected database creation module, a player interface, a data/keystroke capture module, an investigator interface, and a game configuration module. The software provided an 'electronic' footprint of activities undertaken by each player, including searches of particular databases, use of email, use of internet, and use of printer for each system user. Footprint data and communication data were used to verify participants' answers to InSort questions. Players were informed that because they were working in a security sensitive environment they were being monitored at all times. This included digital video recording, keystroke data, and monitoring mobile phone usage (text and voice).

InSort comprised 56 questions, of which 16 were repeated (example questions see appendix A):

- Two questions collected information regarding team membership and role, answered via a drop-down menu.
- One question asked participants to indicate which databases they had access to as a function of their role and team, again via a drop-down menu.
- Three open target questions invited textual responses regarding incident-specific duties, communications activity and movements around the office including access to the printer room and printing activity.

- Eight forced-choice yes/no questions concerned password security and adherence to iCOS rules and regulations regarding data security.

The following yes/no questions were repeated twice, randomly throughout the InSort interview:

- Four related to access to each of the four databases.
- Four concerned attempted (but unsuccessful) access to each of the four databases.
  Four concerned mobile phone usage (1), SMS messaging (1), emailing documents (1), and email behaviour (1).
- Four questions concerned visiting the meeting room, meeting other players, visiting the printer room, and printer use.

Participants received instructions on completing InSort, after which they logged in using a unique identifier. Participants could only move forwards through InSort and were unable to skip questions. On completion, participants provided feedback regarding player strategies, behaviours and perceptions of InSort via a hard copy questionnaire comprising 10 questions with Likert scale (ranging from 1 to 5) or yes/no responses.

This research complied with the American Psychological Association Code of Ethics and was approved by the Lancaster University Institutional Review Board. Informed consent was obtained from each participant (materials are available from the first author).

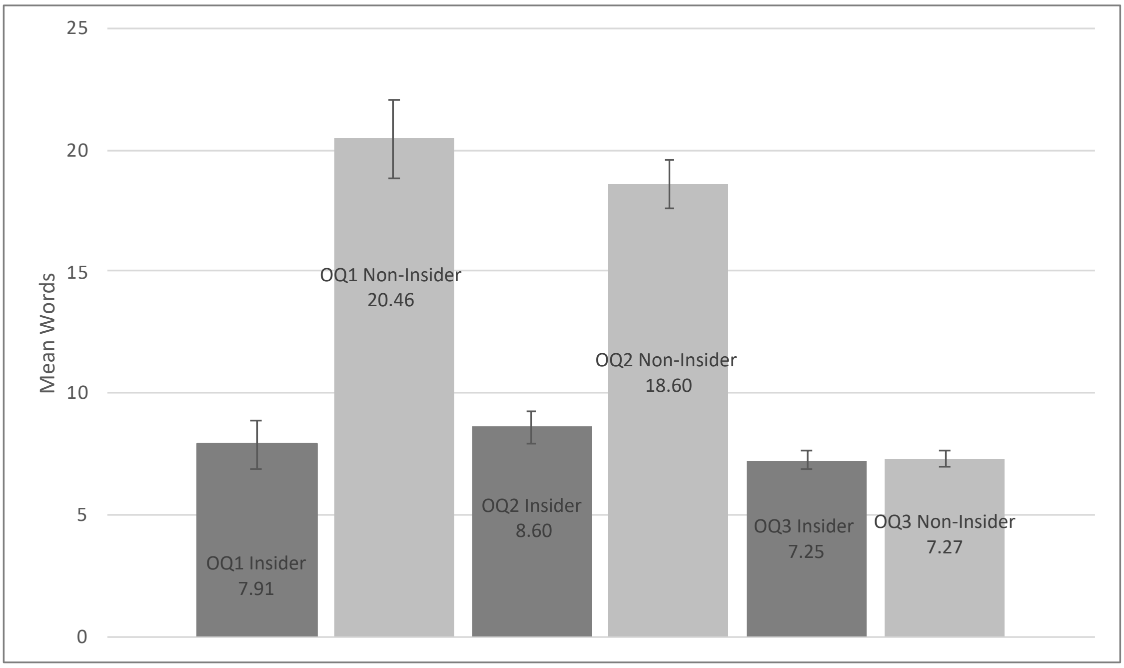
Results

Duration (H[1]). Two-way ANOVAs revealed a significant main effect of group (insider, non-insider) , $F(1, 54) = 187.81$ $p < .001$, $\eta_p^2 = 0.88$. Insiders took twice as long to complete InSort (M = 696s, SD = 120.28, 95% CI, 626.62; 765.52) than non-insiders (M = 340s, SD = 79.37, 95% CI, 316.15; 363.29). Main effects of team (Narcotics, Fraud, Trafficking) and team role (Administrator, Field Agent, Intelligence Analyst, Tactical Investigator) and all interactions were non-significant, as were the all Fs < 0.35, all ps > .097.

Word count and information content (H^2). Two-way ANOVAs revealed a significant main effect of group (insider, non-insider) for the total number of words in response to each open target questions, $F(1, 36) = 12.866$, $p = .001$, $\eta_p{}^2 = 0.26$, and $F(1, 36) = 23.95$, $p < .001$, $\eta_p{}^2 = 0.40$, respectively (see Fig. 1). Non-insiders wrote three times more words (SD = 10.67) than insiders (SD = 2.21) for OQ1 and 2.5 more words (SD = 18.43) for OQ2 than insiders (SD = 8.40). Main effects of team (Narcotics, Fraud, Trafficking) and team role (Administrator, Field Agent, Intelligence Analyst, Tactical Investigator) were non-significant, as were all interactions, all ps > .554 (see Table 1). OQ3 was only available to participants who responded ‘yes’ to questions concerning printer usage, emailing documents for printing and visiting the printer room. Accordingly, 25 participants responded to OQ3, of which seven were insiders (50% of insiders; 30% of non-insiders). A one-way ANOVA revealed no significant difference between insiders and non-insiders for total word count in response to OQ3, $p = .894$ (see Fig. 1).

Figure 1.

Mean word count for each of open question (OQ1, OQ2 and OQ3) as a function of group (insider; non-insider).



Information items in response to open target questions (OQ1, OQ2 and OQ3) were calculated by summing the number of correct, discrete, quantifiable investigation relevant information (IRI) items (see Oxburgh et al., 2012: Philips et al., 2012 for more on IRI). For example, the following response was coded as six information items, *'Over the day I was tasked with looking at conversations* [1] *and other intelligence information in the human trafficking intercepts database* [2]*. I did this to try and track down and formulate an arrest list* [3] *for the leaders of the Zebra gang* [4]*, the Garfunkels gang* [5] *and by working in collaboration with my team members, particularly the tactical investigator* [6]*"*.

Responses to open questions were initially coded by a researcher naïve to the research design and hypotheses following a set of guidelines. 20% (12) of responses from each of the three questions (randomly selected) then underwent independent secondary coding. Inter-rater agreement (IRA) between the coders was high for each of the open questions, r = .916 (OQ1), r = .882 (OQ2) and r = .902 (OQ3).

Two-way ANOVAs revealed significant main effects of group for total information items in OQ1 (individual roles) and OQ2 (individual movements), $F(1, 36) = 9.485$, $p = .003$,

$\eta_p{}^2 = 0.22$ and, $F(1, 36) = 34.75$, $p < .001$, $\eta_p{}^2 = 0.49$, respectively. No other main effects nor interactions emerged, all *p*s > .071. In response to OQ1 and OQ2, insiders provided far less information than non-insiders (see Table 1).

Table 1.

Mean information items for each open question (OQ1, OQ2 and OQ3) as a function of group (insider; non-insider).

	Insider	Non-Insider
	M (95% CI)	
Open Question 1	0.86 (.31: 1.41)	4.30 (3.43: 5.18)
Open Question 2	1.07 (.50: 1.65)	3.85 (3.43: 4.26)
Open Question 3	.86 (.22: 1.50)	1.50 (1.11: 1.89)

Closed target question errors (H³). Answers to each of the questions that comprised the four clusters of closed repeated target questions were scored as correct (awarded 1) or incorrect (awarded 2) at Time 1 (first presentation) and in a similar fashion again at Time 2 (second presentation) resulting in an overall target question consistency score for each participant (lower score indicates fewer errors) per cluster (see Table 2). Answers were scored as correct only if participants responded in accordance with behaviours known to match the electronic footprint and surveillance data. The maximum error score (answered incorrectly at Time 1 & 2) was 16. A score of 8 indicated respondents were correct on both occasions.

Table 2.

Mean target question cluster error scores a function of group (insider; non-insider) where, max. error score = 16, min. = 8.

	Insider	Non-Insider
	M (95% CI)	
Database Accessed	9.93 (9.07: 10.79)	9.45 (9.08: 9.88)
Database Access Attempted	10.43 (9.26: 11.60)	9.52 (9.09: 9.95)
Communication	12.36 (11.15: 13.57)	9.50 (9.05: 9.95)
Movement	8.71 (8.19: 9.24)	8.78 (8.05: 9.03)

Two-way ANOVAs revealed non-significant effects of group, team and team role and non-significant interactions for successful database access target questions, all *p*s > .131. Similarly, target question scores for attempted database access revealed non significant main effects and interactions, all *p*s > .077. A significant main effect of group (insider, non-insider) emerged for target question scores for communication behaviours, $F(1, 36) = 29.268$, $p <$ .001, $\eta_p^2 = 0.45$. Insider's scored higher than non-insiders', indicating discrepancies in responding. All other main effects and interactions were non-significant, all *p*s > .103. Target question scores for the cluster of movement questions revealed non-significant main effects and interactions, all *p*s > .168.

Answer-Evidence Inconsistency (H^3). Answers to closed target questions at Time 1 were scored as consistent (1) or inconsistent (2) with known evidence. Scores were summed, referred to as the *answer-evidence inconsistency scale*, where a lower score indicates higher answer-evidence consistency. Mann-Whitney tests (data violated parametric assumptions) revealed a significant difference between insiders and non-insiders for answer-evidence inconsistency scores, $U = 43.00$, z = - 5.046, $p < .001$, $r = -.084$. Overall, insiders' answer-evidence inconsistency scores were higher (*Mdn* = 22.07) than non-insiders' (*Mdn* = 15.85).

Post InSort Feedback (H^4). All participants reported understanding the InSort instructions and complying with instructions. Insiders (M_{Insiders} =1.93, 95% CI, 1.51: 2.35) reported InSort more demanding ($M_{\text{Non- Insiders}}$ = 3.52, 95% CI, 3.27: 3.78), $F(1, 59) = 39.11$, $p < .001$, $\eta_p^2 = 0.67$, and were less confident that their answers were correct, $F(1, 59) = 45.41$, $p < .001$, $\eta_p^2 = 0.62$ (M_{Insiders} = 4.29, 95% CI, 3.52: 5.05 and $M_{\text{Non insiders}}$ = 2.04, 95% CI, 1.74, 2.34). Insiders reported finding the questions more difficult, $F(1, 59) = 7.22$, $p = .009$, $\eta_p^2 = 0.41$ (M_{Insiders} = 1.50, 95% CI, 1.20: 1.80 and $M_{\text{Non insiders}}$ = 2.11, 95% CI, 1.87, 2.17).

Insiders reported being dishonest when answering questions, X^2 (1, 60) = 19.543, $p <$ .001 and withholding information more often, X^2 (1, 60) = 24.65, $p < .001$. There was no difference between insiders and non-insiders when asked whether InSort questions had been repeated, $p = .634$. Overall, 27 responded (45%) ‘no’, 16 (27%) were ‘unsure’ and 17 (28%) said ‘yes’. Again, no difference emerged between insiders and non-insiders as which types of questions (yes/no or text responses) had been more demanding, $p = .370$. Overall, 25 (42%) reported yes/no questions to be most demanding, 26 (43%) textual responses, and 9 (15%) reported all questions were equally demanding.

Discussion

Insider attacks are increasing in number and magnitude, with potential to undermine national and international security, cause financial loss and reputational damage (e.g., Legg, 2017; Wei et al., 2021). We developed InSort, a text-based synchronous triage with potential for highlighting persons of interest after an insider incident. Insiders took twice as long to complete InSort, were less confident their answers were correct, found InSort more cognitively challenging, provided less information, and typed fewer words. Our results confirm findings of previous research in face-to-face and remote person-to-person contexts that questioning strategies which maximize cognitive burden can amplify signals of deception (e.g., Boggard et al., 2016; DePaulo et al., 2003), highlighting the potential of remote automated CMC.

Open questions increased the information harvested, eliciting an individual's version of the truth, which can be explored for veracity (e.g., Kontogianni et al., 2020; Snook et al., 2010). Tactical questioning, concerning known or verifiable information are spread throughout InSort rather than clustered at the beginning or end, which improves the veracity performance by interviewers and observers (Dando et al., 2015; Levine, 2018). We incorporated both where response time was not constrained, but where response time was monitored. Yet, although respondents could take their time, did not have to consider social context and how their answers/behaviours were received, tactical questioning again leveraged diagnostic indicators across a cohort.

The remote CMC nature of InSort may have diverted impression management towards behaviours perceived by insiders as more important, hence engendering differences in the time taken to complete InSort and in the informational content in open question responses. The absence of a human questioner, and without understanding the importance of *all* response behaviours, some behaviours were attended to at the expense of others. Providing a coherent and consistent narrative without contradictions, with little time to prepare and where questions are not chronologically ordered, may explain the increased duration. Insider responses to open target questions were shorter, suggesting they were seeking to appear credible and cooperative, simultaneously being cautious in responding (see Sporer, 2016; Schuetzler et al., 2019; Zukerman et al., 1981). Wordy replies with low information can be indicative of deception, but not always. However, here short information poor replies were indictive of insiders, possibly being deceptive by withholding information, which is reported in face-to-face contexts (DeRosa et al., 2019; Levine, 2018)

Our findings are consistent with findings regarding the efficacy of automated screening systems for detecting deception at border crossings and in job interviews, further indicating that textual response content and response behaviours are important

(Higginbotham, 2013; Nunamaker et al., 2011; Schuetzler, et al., 2019). Our results are also consistent with cognitive load explanations of deceptive communication (Ho et al., 2016). Creation and then typing of answers to questions is complex and time consuming, but the additional demands associated with being deceptive is more time consuming still. Deceptive textual communications are shorter due to the challenges of drawing multiple responses from memory as plausible answers to questions (e.g., Burgoon et al., 2003; Pollina et al., 2017; Schuetzler et al., 2019).

Manipulative questioning includes repeat questions, which we believed could leverage notable inconsistencies between insiders and non-insiders because insiders would struggle to provide credible and consistent responses to repeat questions (H^3). Our question cluster scores alone did not generally support this hypothesis. However, one important finding was that insiders did not successfully monitor their communication behaviour and so were unable to maintain consistency. Future triage approaches might consider capturing detailed human-human remote interaction behaviours.

Although the consistency across time literature in face-to-face contexts is mixed, our findings suggest deceivers can be as consistent, sometimes more so than truthtellers (e.g., Blair et al., 2018; Clemens & Grolig, 2018; Masip et al., 2018). Conversely, answer-evidence inconsistency scores differed significantly. While insiders were consistent in textual responses, responses to target questions were inconsistent with evidence, which mirrors results in face-to-face contexts (Hartwig et al., 2006; Sukumar et al., 2018). However, here participants were aware their behaviour was monitored throughout and that movement information was collected. In face-to-face contexts participants are often unaware of information known by interviewers, which is fundamental to the success of tactical and strategic interviewing techniques (e.g., see Oleszkiewicz & Watson, 2021). Here, despite knowing behaviour information was collected, answer-evidence inconsistency again emerges as a useful metric with potential for improving veracity decisions.

Information Manipulation Theory 2 (McCornack et al., 2014: IMT2) may be relevant whereby cognitive load is related to difficulty of reasoning through the problem space created bya gap between the initial state, in our study the questions asked by InSort, and the end state (avoidance of detection). IMT2 suggests lies are produced only when the production of the truth is problematic, and that high cognitive load is not intrinsic to deceptive discourse but depends on the potential number of solutions needed to present the version judged most appropriate. Our game was designed to mimic demands experienced by insiders in a secure environment. Hence, there were numerous narratives insiders could choose. IMT2 also proposes quantity violations such as omitting problematic discourse as a frequent form of deceptive discourse. This might explain why insiders produced fewer words.

Limitations and Future Directions

Our simulation embodied some features of organizations, but there are differences between it and the real world. As Taylor et al. (2013) point out the absence of a ‘world’ outside the simulation as a limitation. Employees often communicate with individuals outside their own organization, increasing the heterogeneity of communication and collaborative behaviours. Insiders were chosen at random without controlling/measuring personality, motivation, or personal circumstances, which may not tally with how insiders emerge. More complex simulations could manage these variables. We compared known insiders to co-workers as a first step towards understanding if InSort might leverage differences in textual responses with reference to theories of cognitive load, information manipulation and deception. More research is required to understand how to delineate signal from noise where status is unknown. Finally, the structure of InSort is guided by the applied deception literature and so likely to remain fairly consistent. However, the informational content of questions is dynamic. Ours was bespoke to the iCOS simulation. Constructing an event specific InSort triage depends upon the nature of tasks workers are required and allowed to do day-to-day, the information known to employers, and the insider event itself, which would guide the informational content.

Conclusions

Findings demonstrate the potential of real time remote investigative triage approaches such as InSort. InSort could regularly be implemented on an ad hoc basis as part of in-house security practices following operations or investigations of the nature described here. This may be useful for collating databases of response behaviours such as answer lengths and response times. Such a database may offer additional information alongside the event specific 'footprint' allowing comparisons across incidents. InSort can be constructed and administered by non-specialists and quickly altered as required across incidents. As such, InSort has potential to expedite investigative processes.

Key Points

- Investigating insider attacks is challenging because of the globalisation of organisations and the fact that insiders exploit legitimate access.
- The acknowledged cognitive demands associated with masking illegal insider activity offer opportunities.
- Drawing on cognitive approaches to deception and understanding of deception-conveying features in textual responses we developed InSort, a rapid remote computer mediated triage for highlighting persons of interest.
- InSort identified persons of interest and so could add to existing insider investigative techniques following an insider attack.

- InSort may be particularly relevant given the globalisation of organisations and advancement of information technology whereby employees are dispersed across national and international sites.

Appendix A: Example InSort Questions

Example open question:

1. *'Please explain what your team role entailed'* Answer via free textual response

Example closed non-target questions:

1. *'What team were you assigned too?'* Answer via a forced choice (one choice allowed) drop down menu
2. *'What was your role in the team?'* Answer via a forced choice (one choice allowed) drop down menu

Example closed target questions (multiple responses option):

1. *'Which databases did your team role allow you to access?'* Answer via a drop down menu allowing multiple choices
2. *'Which data bases did you access during the investigation?'* Answer via a drop down menu allowing multiple choices

Example closed target questions (forced choice response):

1. *'Did you attempt to access the 'Shared Network' database?'* Yes/no
2. *Did you share your 'Shared Network' database password with anyone?'* Yes/no

References

Aamodt, M. G., & Custer, H. (2006). Who can best catch a liar? *Forensic Examiner*, *15*(1), 6.

Bhatt, S., Mbwana, J., Adeyemo, A., Sawyer, A., Hailu, A., & Vanmeter, J. (2009). Lying about facial recognition: an fMRI study. *Brain and Cognition*, *69*(2), 382-390.

Blandón-Gitlin, I., Fenn, E., Masip, J., & Yoo, A. H. (2014). Cognitive-load approaches to detect deception: searching for cognitive mechanisms. *Trends in Cognitive Sciences*, *18*(9), 441-444.

Blair, J. P., Reimer, T. O., & Levine, T. R. (2018). The role of consistency in detecting deception: The superiority of correspondence over coherence. *Communication Studies*, *69*(5), 483-498.

Bogaard, G., Meijer, E. H., Vrij, A., & Merckelbach, H. (2016). Strong, but wrong: Lay people's and police officers' beliefs about verbal and nonverbal cues to deception. *PloS One*, *11*(6), e0156615.

Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review*, *10*(3), 214-234.

Burgoon, J. K., Floyd, K., & Guerrero, L. K. (2010). Nonverbal communication theories of interpersonal adaptation. In *The New SAGE Handbook of Communication Science* (pp. 93-110). Sage.

Burgoon, J. K., Blair, J. P., Qin, T., & Nunamaker, J. F. (2003, June). Detecting deception through linguistic analysis. In *International Conference on Intelligence and Security Informatics* (pp. 91-101). Springer, Berlin, Heidelberg.

Chan, S., & Bull, R. (2014). The effect of co-offender planning on verbal deception. *Psychiatry, Psychology and Law*, *21*(3), 457-464.

Chattopadhyay, P., Wang, L., & Tan, Y. P. (2018). Scenario-based insider threat detection from cyber activities. *IEEE Transactions on Computational Social Systems*, *5*(3), 660-675.

Clearswift Insider Threat Index (2017) https://www.clearswift.com/about-us/pr/press-releases/insider-threat-74-security-incidents-come-extended-enterprise-not-hacking-groups

Clemens, F., & Grolig, T. (2019). Innocent of the crime under investigation: Suspects' counter-interrogation strategies and statement-evidence inconsistency in strategic vs. non-strategic interviews. *Psychology, Crime & Law*, *25*(10), 945-962.

Colwell, L. H., Miller, H. A., Lyons Jr, P. M., & Miller, R. S. (2006). The training of law enforcement officers in detecting deception: A survey of current practices and suggestions for improving accuracy. *Police Quarterly*, *9*(3), 275-290.

Colwell, K., Hiscock-Anisman, C. K., Memon, A., Taylor, L., & Prewett, J. (2007). Assessment criteria indicative of deception (ACID): An integrated system of investigative interviewing and detecting deception. *Journal of Investigative Psychology and Offender Profiling*, *4*(3), 167-180.

Costa, D. L., Albrethsen, M. J., & Collins, M. L. (2016). *Insider threat indicator ontology*. https://apps.dtic.mil/sti/citations/AD1044939

CPNI (2020). *Investigation and Disciplinary. https://www.cpni.gov.uk/insider-risks/investigation-disciplinary*

Dando, C. J., & Bull, R. (2011). Maximising opportunities to detect verbal deception: training police officers to interview tactically. *Journal of Investigative Psychology and Offender Profiling*, *8*(2), 189-202.

Dando, C. J., & Ormerod, T. C. (2017). Analyzing decision logs to understand decision making in serious crime investigations. *Human factors*, *59*(8), 1188-1203.

Dando, C. J., & Ormerod, T. C. (2020). Noncoercive human intelligence gathering. *Journal of Experimental Psychology: General*, *149*(8), 1435.

Dando, C. J., Bull, R., Ormerod, T. C., & Sandham, A. L. (2015). Helping to sort the liars from the truth-tellers: The gradual revelation of information during investigative interviews. *Legal and Criminological Psychology*, *20*(1), 114-128.

DePaulo, B.M., Lindsay, J.J., Malone, B.E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin*, *129*(1), 74-118.

De Rosa, J., Hiscock-Anisman, C., Blythe, A., Bogaard, G., Hally, A., & Colwell, K. (2019). A comparison of different investigative interviewing techniques in generating differential recall enhancement and detecting deception. *Journal of Investigative Psychology and Offender Profiling*, *16*(1), 44-58.

Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020, June). Evaluation of machine learning algorithms for anomaly detection. In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.

European Union Agency for Cybersecurity (2020) Threat Landscape 2020 - Insider threat. https://www.enisa.europa.eu/publications/insider-threat

Fenn, E., McGuire, M., Langben, S., & Blandón-Gitlin, I. (2015). A reverse order interview does not aid deception detection regarding intentions. *Frontiers in Psychology*, *6*, 1298.

Fisher, R. P., & Geiselman, R. E. (2010). The cognitive interview method of conducting police interviews: Eliciting extensive information and promoting therapeutic jurisprudence. *International Journal of Law and Psychiatry*, *33*(5-6), 321-328.

Granhag, P. A., & Hartwig, M. (2015). The strategic use of evidence technique: A conceptual overview. *Detecting deception: Current challenges and cognitive approaches*, 231-251.

Greitzer, F., Purl, J., Leong, Y. M., & Becker, D. S. (2018, May). Sofit: Sociotechnical and organizational factors for insider threat. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 197-206). IEEE.

Hamlin, I., Taylor, P. J., Cross, L., MacInnes, K., & Van der Zee, S. (2020). A psychometric investigation into the structure of deception strategy use. *Journal of Police and Criminal Psychology*, 1-11.

Hartwig, M., Granhag, P. A., Stromwall, L., Wolf, A. G., Vrij, A., & Hjelmsäter, E. R. A. (2011). Detecting deception in suspects: Verbal cues as a function of interview strategy. *Psychology, Crime & Law*, *17*(7), 643-656.

Hartwig, M., Granhag, P. A., Strömwall, L. A., & Kronkvist, O. (2006). Strategic use of evidence during police interviews: When training to detect deception works. *Law and Human Behavior*, *30*(5), 603-619.

Hauch, V., Sporer, S. L., Michael, S. W., & Meissner, C. A. (2016). Does training improve the detection of deception? A meta-analysis. *Communication Research*, *43*(3), 283 343.

Ho, S. M., Hancock, J. T., Booth, C., & Liu, X. (2016). Computer-mediated deception: Strategies revealed by language-action cues in spontaneous communication. *Journal of Management Information Systems*, *33*(2), 393-420.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1-40.

Intel Security (2015). Grand Theft Data. Data exfiltration study: Actors, tactics, and detection. https://cdn2.hubspot.net/hubfs/3375090/Nukon_June2017-theme/Pdf Files/rp-data-exfiltration.pdf

Jenkins, M. C., & Dando, C. J. (2012). Computer-mediated investigative interviews: A potential screening tool for the detection of insider threat. In *Proceedings of the 10th Biennial Conference of the International Conference of Forensic Linguistics, Birmingham: Center for Forensic Linguistics*.

Jiang, W., Liu, H., Zeng, L., Liao, J., Shen, H., Luo, A., ... & Wang, W. (2015). Decoding the processing of lying using functional connectivity MRI. *Behavioral and Brain Functions*, *11*(1), 1-11.

Jensen, C. S., Prasad, M. R., & Møller, A. (2013). Automated testing with targeted event sequence generation. In *Proceedings of the 2013 International Symposium on Software Testing and Analysis* (pp. 67-77).

Kohan, M. D., Nasrabadi, A. M., & Shamsollahi, M. B. (2020). Interview based connectivity analysis of EEG in order to detect deception. *Medical Hypotheses*, *136*, 109517.

Kontogianni, F., Hope, L., Taylor, P. J., Vrij, A., & Gabbert, F. (2020). "Tell me more about this…": An examination of the efficacy of follow-up open questions following an initial account. *Applied Cognitive Psychology*, *34*(5), 972-983.

Lee, C. C., Welker, R. B., & Odom, M. D. (2009). Features of computer-mediated, text-based messages that support automatable, linguistics-based indicators for deception detection. *Journal of Information Systems*, *23*(1), 5-24.

Legg, P. A. (2017). Human-machine decision support systems for insider threat detection. In *Data Analytics and Decision Support for Cybersecurity* (pp. 33-53). Springer, Cham.

Levine, T. R. (2018). Scientific evidence and cue theories in deception research: reconciling findings from meta-analyses and primary experiments. *International Journal of Communication*, *12*, 19.

Levine, T. R. (2014). Truth-default theory (TDT) a theory of human deception and deception detection. *Journal of Language and Social Psychology*, *33*(4), 378-392.

Levine, T. R., Blair, J. P., & Carpenter, C. J. (2018). A critical look at meta-analytic evidence for the cognitive approach to lie detection: A re-examination of Vrij, Fisher, and Blank (2017). *Legal and Criminological Psychology*, *23*(1), 7-19.

Lew, Z., Walther, J. B., Pang, A., & Shin, W. (2018). Interactivity in online chat: Conversational contingency and response latency in computer-mediated communication. *Journal of Computer-Mediated Communication*, *23*(4), 201-221.

Markowitz, D. M. (2020). The deception faucet: A metaphor to conceptualize deception and its detection. *New Ideas in Psychology*, *59*, 100816.

Masip, J., Martínez, C., Blandón-Gitlin, I., Sánchez, N., Herrero, C., & Ibabe, I. (2018). Learning to detect deception from evasive answers and inconsistencies across repeated interviews: A study with lay respondents and police officers. *Frontiers in Psychology*, *8*, 2207.

Maybury, M. (2006). *Detecting malicious insiders in military networks*. Mitre Corp. Bedford MA.https://apps.dtic.mil/sti/pdfs/ADA456254.pdf

Matsumoto, D., Hwang, H. S., Skinner, L., & Frank, M. (2011). Evaluating truthfulness and detecting deception. *FBI L. Enforcement Bull.*, *80*, 1.

McCornack, S. A., Morrison, K., Paik, J. E., Wisner, A. M., & Zhu, X. (2014). Information manipulation theory 2: A propositional theory of deceptive discourse production. *Journal of Language and Social Psychology*, *33*(4), 348-377.

Meissner, C. A., & Lyles, A. M. (2019). IX investigations: The importance of training investigators in evidence-based approaches to interviewing. *Journal of Applied Research in Memory and Cognition*, *8*(4), 387-397.

Mills, J. U., Stuban, S. M., & Dever, J. (2017). Predict insider threats using human behaviors. *IEEE Engineering Management Review*, *45*(1), 39-48.

National Law review (2020). Frequency and Cost of Insider Threats Continue to Increase.https://www.natlawreview.com/article/frequency-and-cost-insider-threats-continue-to-increase

Nortje, A., & Tredoux, C. (2019). How good are we at detecting deception? A review of current techniques and theories. *South African Journal of Psychology*, *49*(4), 491-504.

Ormerod, T. C., & Dando, C. J. (2015). Finding a needle in a haystack: Toward a psychologically informed method for aviation security screening. *Journal of Experimental Psychology: General*, *144*(1), 76.

Oleszkiewicz, S., & Watson, S. J. (2021). A meta-analytic review of the timing for disclosing evidence when interviewing suspects. *Applied Cognitive Psychology*, *35*(2), 342-359

Oxburgh, G., Ost, J., & Cherryman, J. (2012). Police interviews with suspected child sex offenders: does use of empathy and question type influence the amount of investigation relevant information obtained?. *Psychology, Crime & Law*, *18*(3), 259-273.

Pang, A., Shin, W., Lew, Z., & Walther, J. B. (2018). Building relationships through dialogic communication: organizations, stakeholders, & computer-mediated communication. *Journal of Marketing Communications*, *24*(1), 68-82.

Parkhouse, T.P. and Ormerod, T.C. (2018). Unanticipated questions can yield unanticipated outcomes in investigative interviews *PLoS ONE*, 13 (12). e0208751.

Pentland, S. J., Twyman, N. W., Burgoon, J. K., Nunamaker Jr, J. F., & Diller, C. B. (2017). A video-based screening system for automated risk assessment using nuanced facial features. *Journal of Management Information Systems*, *34*(4), 970-993.

Phillips, E., Oxburgh, G., Gavin, A., & Myklebust, T. (2012). Investigative interviews with victims of child sexual abuse: The relationship between question type and investigation relevant information. *Journal of Police and Criminal Psychology*, *27*(1), 45-54.

Pollina, D. A., Woods, R. J., Salyer, C. D., Leffingwell, T. G., Cooper, C., & Rohrbaugh, J. W. (2017). Verbal response time and duration indices of deception in humans interviewed by a computer-generated agent. *International Journal of Human-Computer Studies*, *97*, 23-33.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *Mis Quarterly*, 1189-1210.

Rubin, V. L., Conroy, N. J., & Chen, Y. (2015). Towards news verification: Deception detection methods for news discourse. In *Hawaii International Conference on System Sciences* (pp. 5-8).

Sánchez-Junquera, J., Villasenor-Pineda, L., Montes-y-Gómez, M., Rosso, P., & Stamatatos, E. (2020). Masking domain-specific information for cross-domain deception detection. *Pattern Recognition Letters*, *135*, 122-130.

Sandham, A. L., Dando, C. J., Bull, R., & Ormerod, T. C. (2020). Improving professional observers' veracity judgements by tactical interviewing. *Journal of Police and Criminal Psychology*, 1-9.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460.

Schuetzler, R. M., Grimes, G. M., & Giboney, J. S. (2019). The effect of conversational agent skill on user behavior during deception. *Computers in Human Behavior*, *97*, 250-259.

Spitzner, L. (2003). Honeypots: Catching the insider threat. In *19th Annual Computer Security Applications Conference, 2003. Proceedings.* (pp. 170-179). IEEE.

Sporer, S. L. (2016). Deception and cognitive load: Expanding our horizon with a working memory model. *Frontiers in Psychology*, *7*, 420.

Sukumar, D., Wade, K. A., & Hodgson, J. S. (2018). Truth-tellers stand the test of time and contradict evidence less than liars, even months after a crime. *Law and Human Behavior*, *42*(2), 145.

Taylor, P. J., Dando, C. J., Ormerod, T. C., Ball, L. J., Jenkins, M. C., Sandham, A., & Menacere, T. (2013). Detecting insider threats through language change. *Law and Human Behavior*, *37*(4), 267.

Trzeciak, R. (2019). *SEI Cyber Minute: Insider Threat Mitigation, We can help!*. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Twyman, N. W., Lowry, P. B., Burgoon, J. K., & Nunamaker Jr, J. F. (2014). Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. *Journal of Management Information Systems*, *31*(3), 106-137.

Vendemia, J., Buzan, R. F., & Simon-Dack, S. L. (2005). Reaction time of motor responses in two-stimulus paradigms involving deception and congruity with varying levels of difficulty. *Behavioural Neurology*, *16*(1), 25-36.

Vredeveldt, A., van Koppen, P. J., & Granhag, P. A. (2014). The inconsistent suspect: A systematic review of different types of consistency in truth tellers and liars. *Investigative Interviewing*, 183-207.

Vrij, A., Granhag, P. A., & Porter, S. (2010). Pitfalls and opportunities in nonverbal and verbal lie detection. *Psychological Science in the Public Interest*, *11*(3), 89-121.

Vrij, A., Meissner, C. A., Fisher, R. P., Kassin, S. M., Morgan III, C. A., & Kleinman, S. M. (2017). Psychological perspectives on interrogation. *Perspectives on Psychological Science*, *12*(6), 927-955.

Wei, Y., Chow, K. P. P., & Yiu, S. M. (2021). Insider Threat Prediction Based on unsupervised Anomaly Detection Scheme for Proactive Forensic Investigation. *Digital Investigation*.

Walczyk, J. J., Grifith, D. A., Yates, R., Visconte, S., & Simoneaux, B. (2013). Eye movements and other cognitive cues to rehearsed and unrehearsed deception when interrogated about a mock crime. *Applied Psychology in Criminal Justice*, *9*(1). 1-23.

Walsh, D., Dando, C. J., & Ormerod, T. C. (2018). Triage decision-making by welfare fraud investigators. *Journal of Applied Research in Memory and Cognition*, *7*(1), 82-91.

Weiss, B., & Feldman, R. S. (2006). Looking good and lying to do it: Deception as an impression management strategy in job interviews. *Journal of Applied Social Psychology*, *36*(4), 1070-1086.

Yao, M. Z., & Ling, R. (2020). “What is computer-mediated communication?” *Journal of Computer-Mediated Communication*, *25*(1), 4-8.

Zhou, L., Burgoon, J. K., Nunamaker, J. F., & Twitchell, D. (2004). Automating linguistics-based cues for detecting deception in text-based asynchronous computer-mediated communications. *Group Decision and Negotiation*, *13*(1), 81-106.

Zuckerman, M., DePaulo, B. M., & Rosenthal, R. (1981). Verbal and nonverbal communication of deception. *Advances in Experimental Social Psychology*, 14, pp. 1-59.

Biographies:

Prof Coral J. Dando is a Professor of Forensic Psychology, at the University of Westminster, London. She has a PhD in Applied Cognition, awarded in 2011 by London South Bank University. Prior to completing her PhD, Coral served as a London police officer for over 10 years.

Prof. Paul J. Taylor is a Professor of Psychology at Lancaster University, UK He has a PhD in Psychology, awarded in 2004 by the University of Liverpool, UK. He is currently the National Scientific Advisor for Policing. Paul was previously the Director of the UK's hub for behavioural and social science for national security.

Prof Thomas C. Ormerod is a Professor of Psychology at the University of Sussex, UK. He has a PhD in Human Computer Interaction, awarded in 1988 by the University of Sunderland, UK. Tom has previously been Head of the School of Psychology at University of Sussex.

Prof Linden Ball is a Professor of Psychology in the School of Psychology and Computer Science at the University of Central Lancashire (UCLan). He has a PhD in Cognitive Processes in Engineering Design, awarded in 1988 by the South West Polytechnic, Plymouth. Linden is Director of Research and Enterprise in the Faculty of Science and Technology and Deputy Director of the UCLan Research Centre for Brain and Behaviour.

Dr Alexandra Sandham is a Senior Lecturer in the Psychology Dept. at the University of Gloucestershire, UK. She has a PhD in Hypothesis Generation in Investigative Contexts, awarded 2012 by Lancaster University. Alexandra has previously worked as a Principal Psychologist at the UK Ministry of Defence.

Mr Tarek Menacere is a software developer. He is currently a Software Developer for Sky. Tarek was previously employed at Lancaster University.