Accepted manuscript of: Searle, R., Renaud, K., & van der Werff, L. (2024). Shaken to the core: trust trajectories during aftermaths of adverse cyber events. Journal of Intellectual Capital. Advance online publication. https://doi.org/10.1108/JIC-02-2024-0038

Shaken to the Core: Trust Trajectories in the Aftermaths of Adverse Cyber Events

Rosalind Searle[1] and Karen Renaud[2] and Lisa van der Werff[3]
[1]rosalind.searle@glasgow.ac.uk, [2]karen.renaud@strath.ac.uk [3] lisa.vanderwerff@dcu.ie,
[1]University of Glasgow
[2]University of Strathclyde, University of South Africa; Rhodes University, Abertay University
[3]Dublin City University

Abstract

Design/methodology/approach: Drawing on pertinent theory and reports of empirical studies, we outline the basis of two alternative subsequent trajectories, drawing out the relationships between trust, vulnerability and emotion, both positive and negative, in the aftermath of an adverse cyber event.

Purpose: Adverse cyber events, like death and taxes, have become inevitable. They are an increasingly common feature of organisational life. Their aftermaths are a critical and under-examined context and dynamic space within which to examine trust. In this paper, we address this deficit.

Findings: We combine stage theory and social information processing theories to delineate the dynamics of trust processes and their multilevel trajectories during adverse cyber event aftermaths. We consider two response trajectories to chart the way vulnerability arises at different levels within these social systems to create self-reinforcing trust and distrust spirals. These ripple out to impact multiple levels of the organisation by either amplifying or relieving vulnerability.

Research Implications: The way adverse cyber events aftermaths are managed have immediate and long-term consequences for organisational stakeholders. Actions impact resilience and ability to preserve the social fabric of the organisations. Subsequent trajectories can be 'negative' or 'positive'. The 'negative' trajectory is characterised by efforts to identify and punish the employee whose actions facilitated the adverse events i.e. the 'who'. Public scapegoating might follow thereby amplifying perceived vulnerability and reducing trust across the board. By contrast, the 'positive' trajectory relieves perceived vulnerability by focusing on, and correcting, situational causatives. Here, the focus is on the 'what' and 'why' of the event.

1 Introduction

Organisations are increasingly reliant on the internet increasing their 'attack surface', exacerbating vulnerability to Adverse Cyber Events (referred to as AdvEvents from now on). These significantly disrupt operations and are costly to recover from (Federal Bureau of Investigation, 2020; Johns, 2020; GOV.UK, 2022). Recent cyberattacks have disrupted the provision of health care e.g., Medibank (Taylor, 2022; Milmo, 2022), transport e.g., Uber (McCallum, 2022), social media e.g., Twitter (Vallance, 2023), education (BBC, 2023), and financial services (Davies, 2023) revealing critical and ongoing vulnerabilities for millions of employee and customer personal records and proprietary commercial information (Claburn, 2022).

AdvEvent aftermaths are characterised by ambiguity regarding 'fault', which manifests in wide-ranging interpretations and perspectives (Arthur, 2018). Suppositions trigger responses and courses of action from the individual 'insider' and other organisational stakeholders, including those in cybersecurity, supervisory and critical leadership roles. Practical advice offered to organisations and their leaders on coping with AdvEvent aftermaths typically focuses on technical vulnerabilities (Ammi et al., 2022; Staves et al., 2022), but seldom mentions this complex interplay and the ensuing dynamics of vulnerabilities (Densham, 2015). The salience of vulnerability and blame attribution (Renaud et al., 2021a), as well as the interpersonal nature of the way organisations react to AdvEvents, means that trust, while central, is often overlooked.

Managing AdvEvent aftermaths requires the attention of senior organisational executives (Garcia-Perez et al., 2023). In processing post-event aftermaths, they have to balance competing attentional *foci.* The actions and reactions of key organisational actors provide important signals and cues for internal and external actors regarding multi-level trust as they make the vulnerability of organisational individual actors either more or less salient (Salancik and Pfeffer, 1978).

The cybersecurity context is often laden with negative emotional experiences (Cram et al., 2024) from compliance with prevention measures (Renaud and Dupuis, 2019) to the more intense impact of AdvEvents [Redacted]. Triggered negative emotions can make it more difficult for people to function effectively (Fredrickson et al., 2003). Anxiety and fear arise from perceived threat or harm from the experience itself, and more critically from ruminating about culpability and potential implications, which could include a reprimand or being laid off BBC (2019). Such rumination influences job engagement and well-being (Kinnunen et al., 2017).

AdvEvents should be processed productively and helpfully (Dalal et al., 2022). Integrating a social science perspective will help organisations to understand how post-event actions influence vulnerability [Redacted] and ultimately their capacity to thrive following a negative event. We contend that a trust-informed approach can render an organisation more resilient against further AdvEvents.

In this paper, we compare two distinct response trajectories, contrasting their dynamics and implications for vulnerability and trust at different levels of organisations. We integrate stage theory (Mohr, 1982) and Social Information Processing (SIP) theory (Salancik and Pfeffer, 1978) with the literature on trust preservation (Gustafsson et al., 2020), to develop a theory of the complicated interplay between trust, emotion and vulnerability.

We develop a theory regarding how early actions and interpretations of AdvEvents produce ripple effects of vulnerability and trust in the organisation as knowledge of the initial breach and response spreads. We highlight how vulnerability can become a salient concern motivating active sense-making and processing of trust requiring a conscious exploration and re-(evaluation) of trust signals (Weibel et al., 2023). If mismanaged, with traditional prioritisation of technical remedies (Joyce, 2022) and outdated management approaches (Howlett, 2020), trust can be breached and destroyed, creating immediate and future negative outcomes for individuals and the organisation as a whole. We make four contributions to the literature:

First, extend the cybersecurity literature by using trust as a lens to advance conceptual understanding of the social ramifications of AdvEvents.

Second, make two important theoretical contributions to the literature on trust (Legood et al., 2023), following the recommendations of Cram et al. (2024) in examining behaviours over time. We also respond to calls from trust scholars (Korsgaard and Bliese, 2021) to build conceptual insights into trust dynamics and their distinct trajectories. We integrate theories of stage theory (Mohr, 1982) and SIP theory (Salancik and Pfeffer, 1978; Van Kleef, 2009), to explore the event spaces of anchoring organisational AdvEvents (Ballinger and Rockmann, 2010) and advance conceptual understanding of how self-reinforcing spirals of vulnerability and trust can emerge and then ripple out through increasingly wider groups of organisational stakeholders.

Third, extend knowledge of trust antecedents by considering reactions to AdvEvents as social spaces in which the actions and emotional displays of key stakeholders influence the extent to which vulnerability and trust are salient concerns. Cues from these social contexts shape both the way in which we trust, the attention devoted to trust information search, and expands knowledge of the cues that drive trust within organisations. In this way, we extend previous work on trust as an active process (Gustafsson et al., 2020; Weibel et al., 2023).

Fourth, we contend that emotional displays by the individual are social cues that facilitate the transition through aftermath stages, and most notably during the reveal stage (Salancik and Pfeffer, 1978). SIP theory indicates that while the individual may believe they control all aspects of disclosure, their emotional reactions may cue others that something untoward has occurred.

Section 2 defines key terms and interrogates the Sony data breach to demonstrate the way the aftermath of AdvEvents are characterised by stages. Section 3 outlines the theory development. Section 4 discusses the implications, limitations and future work. Section 5 concludes.

2 Key Concepts & Aftermath Stages

The term **AdvEvent** denotes events: (1) originating from the actions of external bad actors (e.g., data breach (Wilson, 2022)); (2) those caused by human error (e.g., forgetting to activate a secure network connection (Vock, 2024)); (3) those caused by an employee falling for a social engineering attack (e.g., Phishing message/AI-powered attack (Vatsa, 2024)). AdvEvents often involve the interaction of individuals across various levels of organisations (Garcia-Perez et al., 2023).

The most common AdvEvent is caused by Phishing (Deloitte, 2020), which can be defined as: "*a scalable act of deception whereby impersonation is used to obtain information from a target*" (Lastdrager, 2014, p. 1). Phishing emails appear to come from a known individual in order to deceive employees into compromising the organisation's systems, so that data can be stolen and held to ransom (ransomware) or encrypted so that the organisation's own access is blocked (Nakashima and Rucker, 2017).

Trust can be defined as "*a psychological state that compromises the willingness to be vulnerable based upon positive expectations of the intentions or behaviours of another party*"(Mayer et al., 1995). Inherent to this commonly accepted definition of **trust** is the concept of *vulnerability* arising from risk and (inter)dependence of trust-relevant situations.

Vulnerability is: "*a perception or feeling that one is exposed to harm or loss*" (Fulmer and Gelfand, 2012).

Trauma stems from harm and denotes the negative consequences and impairment of well-being for the subject of harm (Agrafiotis et al., 2018). Types of harm include: psychological relating to the individual's psyche and well-being [Ibid].

Stage theories are triggered by a particular event, a discrete episode, which is at the core of our experiences of daily personal and organisational life. Building on open systems theory (Katz and Kahn, 1978), Morgeson *et al.* define events as "*external, bounded in time and space and involving the intersection of different entities*" (Morgeson et al., 2015, p. 520). They can arise at any level in an organisation's hierarchy, with effects remaining at the origin level, or transcending to other levels. Within the context of cybersecurity, the triggering salient event is likely to be the realisation that the AdvEvent has occurred and that they may have triggered it. Employees progress through a number of stages as the aftermath period unfolds. This is when the vulnerability of involved individuals, and the organisation itself, is foregrounded, which creates a period of more active and systematic processing of trust (Gustafsson et al., 2020; Weibel et al., 2016).

2.1 AdvEvent Aftermath Stages

In the trust recovery context (not necessarily related to AdvEvents), other researchers have identified specific stages that characterise the employee's journey. For example, Pfarrer et al. (2008) propose a four-stage model of recovery after a transgression, comprising: (1) discovery, (2) explanation, (3) penance, and (4) rehabilitation. Gillespie and Dietz (2009) also suggested a four-stage model of trust repair after a transgression: (1) immediate response, (2) diagnosis, (3) reforming interventions, and (4) evaluation. In both models, the first stage is triggered by an individual reporting a transgression and the initial response from the person they report to. It is perhaps best referred to as a 'REVEAL' stage. The next stage brings other parties into play, and often involves others trying to decide who is responsible for the AdvEvent or transgression. This is the 'REACTION' stage. A third stage occurs as all stakeholders try to get back to normal. We will refer to this as 'RESTABILISATION'.

These studies analysed situations where transgressors are employees. We are studying the aftermath of an AdvEvent. As such, it is worth noting that in the cyber domain, an AdvEvent is usually due to the actions of an external actor. In many cases, the insecure behaviours of an internal employee unwittingly facilitated the hacker's ingress into the organisations' systems. This being so, it might take some time for an internal actor to realise that a breach has occurred, and that it happened because of their own negligence or naivety. Hence, we need a stage that precedes the reveal stage, called 'REALISATION', for AdvEvents in the cyber domain.

Learning from an Actual Organisation

We now examine an actual cybersecurity AdvEvent, and its aftermath, to confirm the stages mentioned in the previous section. Sony became a target of a North Korean perpetrated a cyberattack following their movie about its leader (Siboni and Siman-Tov, 2014). We now examine the Sony breach because impacts on staff are comprehensively reported, which allows us to delineate particular stages that characterise the aftermath.

Other researchers argued for the suitability of the Sony case in terms of exploring impacts on employees given that for this case, unusually, media reports covered these stakeholders (Agrafiotis et al., 2018). We confirm that the aftermath is characterised by activities in four stages, reflecting step changes in employees' perceptions and feelings.

Stage 1: Initial Breach: REALISATION: Lee (2014) reports that when Sony employees arrived at work on 24 November 2014, they discovered that the corporate network was unavailable. This period was characterised by uncertainty, with staff being told to work on whiteboards but not being given details about what the problem was. They were not told what had happened nor what actions were being taken to remedy the situation. A sense of vulnerability was heightened based on a concern about their own personal and financial details had potentially been leaked during the breach (Agrafiotis et al., 2018).

Stage 2: Beyond individuals to Community: REVEAL: Arthur (2018) reports that, *on the day after the Sony attack*, the FBI held information sessions during which employees were lectured about password "best practice" and spotting phishing attacks. There was speculation that a disgruntled employee could have been behind a hack of the organisation (Hamedy and Faughnder, 2015). The finger of blame was already searching for a culpable employee. On the 5th December, some Sony employees received a threatening email from an individual claiming to be a member of the hacking group (Villarreal, 2014). It instructed them to disassociate themselves from Sony.

Psychological harms arose from hackers' direct emails to employees threatening their families if they failed to call Sony out. The selling of their financial details on the dark web led to the raiding of some personal bank accounts (Agrafiotis et al., 2018). Further, vulnerability arose from leaks that exposed Sony's diversity issues to the press (Hess, 2015). Hess (2015) reports that, despite provision of psychological counselling for employees, several key employees left the company.

Stage 3: Beyond Community to Organisation: REACTION (3 weeks after): On the 15th December, staff were told that the hacking would not take Sony down. They were told not to be worried about the future of the studio (Faughnder, 2014). However, it is clear that staff did not believe this, because on the very next day, lawyers filed two class-action lawsuits on behalf of employees who alleged negligence by Sony (Hamedy and James, 2014). Analysts started to wonder how long Sony's Chairman Michael Lynton and co-Chairman Amy Pascal could survive (Battaglio and Verrier, 2014). There were calls for 'new leadership'.

Stage 4: RESTABILISATION: A new CEO was appointed (3 months later). Tom Rothman replaced Pascal as head of Sony's studio (Faughnder, 2015). Sony reached a settlement with current and former employees. They paid up to $8 million to reimburse employees for identity-theft losses, preventative measures and legal fees related to the hack (Associated Press, 2015).

2.2 Takeaways

This case study demonstrates:

- An **AdvEvent's aftermath** progresses through four distinct **stages** as employees and management grapple with what has occurred.
- The **way people are treated** is key. In the Sony case, management seemed oblivious to this and ended up paying out millions based on a class action suit. The Equifax breach of 2017 provides us with a good example (Weise, 2024). Within a week of the breach being announced, Equifax announced that its chief information officer, and chief security officer were retiring immediately. Eleven days later, the CEO also retired. One can only imagine what occurred in the organisation to precipitate this.

  An example of poor staff treatment is borne out by a post by an anonymous employee in an unnamed organisation who mistakenly uploaded the wrong document to a client. He was given a verbal warning (Anonymous, 2021). In posting, he was asking for advice, and responsive comments are instructive. One said: "*Be proactive and responsible – you could use this opportunity to strengthen your relationship with your employers and build a more trusting relationship.*" This response acknowledges the loss of trust the anonymous poster suffered.
- **Trust variations occur at all levels of the organisation** as people traverse the different stages. It is interesting that Sony's initial reactions demonstrated a lack of trust in their own staff. In the SolarWinds data breach case, the organisation attempted to blame an intern for what had occurred (Lakshmanan, 2021). Such obvious attempts to scapegoat will exacerbate vulnerability (Gentry, 2015).

We were unable to find documented examples of data breaches that were well managed, such that vulnerability was relieved and trust enhanced. It is likely that these cases do not reach the newspapers because employees do not come into conflict with their employers.

During an industry engagement event, the third author was told about an event where an employee clicked on a Phishing message and realised what she had done. She contacted the security team, who thanked her and acted immediately to investigate and mitigate. She was not humiliated nor shamed in front of her peers. The employee was not afraid to report because the organisation fostered a no-blame culture. This is admittedly an anecdote, but does provide some evidence that there are organisations who deliberately enhance trust in managing AdvEvents

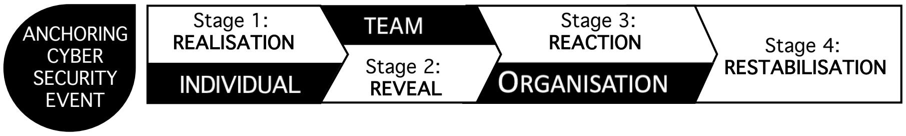

Figure 1: Adverse Cybersecurity Event Aftermath Stages

Based on these insights, we use the staged model (Siponen, 2024; Mohr, 1982) shown in Fig. 1 to structure the discussion to answer the following research question: **"How do changes in trust levels influence the organisation's future viability?"**

3 Theory Development

Attempts are increasingly made to reduce cyber risks from employee actions by means of cybersecurity awareness training programmes and compliance mandates. cyberattacks often deliberately target deficits in employee security awareness (Ng et al., 2021). However, even knowledgeable staff can be deceived (De Luca et al., 2016) and respond unwisely to messages that are carefully designed to elicit responses. Many will appear to come from their leaders (referred to as 'Whaling') (Pienta et al., 2020), applying pressure to trigger a rapid response (Vatsa, 2024).

Despite considerable ambiguity, attributing cause and responsibility for events like these has critical implications for trust levels within organisations. When enabling insiders are deceived into allowing an attacker access to their organisation, their willingness to be vulnerable to the purported sender of the email is deliberately exploited by a third party. They are unlikely to have a pre-existing relationship with the actual email sender, nor any insight into the fact that this might be a cyberattack. Otherwise, they would not render themselves vulnerable by trusting the email. However, these events represent an interesting trust dilemma for the enabling insider as they are both a victim to the malicious unknown party and the enabler of a potentially serious crime against their organisation.

Although previous literature has focused primarily on the positive expectations aspect of the trust definition, our intention is to consider how willingness to be vulnerable might evolve over time following a AdvEvent. In particular, we are initially interested in how the enabling insider is likely to perceive their own changing vulnerability. Further, how other key stakeholders impact this experience and the creation of a ripple effect that influences the extent to which other employees are willing to make themselves vulnerable in this evolving organisational environment. Hence, we chart the emergence and dynamics of trust in this context (Korsgaard and Bliese, 2021).

3.1 Social Information Processing (SIP) following an AdvEvent

In theorising about trust in the aftermath of cybersecurity breaches, we integrate two theoretical frameworks, stage theory (Mohr, 1982) and SIP theories (Salancik and Pfeffer, 1978), to advance insights into how the aftermath is experienced and processed.

Although trust can potentially cost the truster dearly (Deutsch, 1958), individuals are motivated to accept vulnerability to parties, including colleagues and their employing organisation ,for instrumental reasons related to access to resources, and also for more intrinsic reasons such as feeling connected and identifying with others (van der Werff et al., 2019). Their willingness to be vulnerable can deliver important benefits (Deutsch, 1958). Govier (1994) suggests that vulnerability arises from: (i) motives, (ii) malfeasance intentions, and (iii) the magnitude of damage produced. Contexts within which vulnerability is more germane include novel situations (McKnight et al., 1998), or the aftermath of specific events, such as a period of crisis (Rice and Searle, 2022) or earlier betrayal (Dirks et al., 2009). Here, we consider employee experiences of vulnerability in the aftermath of an AdvEvent, exploring the way the event and aftermath triggers an active search for, and processing of, information pertaining to trust that can fundamentally alter ongoing future social interactions (Misztal, 2012).

SIP theory contends that perceptions and decisions about how we should act are shaped by the social networks and organisational contexts within which we are embedded (Salancik and Pfeffer, 1978). Our social environment provides us with a host of social cues that help us understand events that occur and how we should respond (Lemerise and Arsenio, 2000) These influence individual and social behaviours, filtering what information is attended to, and providing interactive sense-making resulting in shared beliefs and attitudes (Searle and Rice, 2024). Our experience of emotions (Damasio, 1994), social norms and the behaviours of others (Salancik and Pfeffer, 1978) in these situations shape what is attended to and allow us to narrow both: (1) the amount of information we need to process, and (2) the number and kinds of possible responses (Lemerise and Arsenio, 2000).

The critical and disruptive nature of AdvEvents adds an intense emotional tone that plays a key role in how we respond to important events (Ballinger and Rockmann, 2010). These can concern individual psychological harm or those from the associated social disruptions (Agrafiotis et al., 2018). Specifically, our own emotions shape our perceptions and motivate particular behaviours, while the emotions of others can change how we ourselves feel and form important social cues as to what we can expect from others (Lerner et al., 2015; Van Kleef, 2014).

These effects are not isolated to the enabling individual and their immediate colleagues. Responses to AdvEvents occur in the broader social space of the organisation and consequences extend beyond initial responses, creating further financial and reputational harms (Agrafiotis et al., 2018). How the enabling individual is treated provides important cues that can ripple out through the wider organisational community.

In the following section, we apply SIP theory to develop an stage model of the multi-level responses and effects of an AdvEvent. We explain how they traverse the four stages that emerged from our case study. Throughout these stages, we expect processing of trust and vulnerability cues to be effortful and systematic as a widening pool of organisational stakeholders becomes more conscious of their vulnerability within this organisation and monitors how the unfolding events are being managed. As a result, during this time we would expect significant changes in levels of trust, and potentially, distrust (Weibel et al., 2023).

3.2 Aftermath Stages

Fig. 4 depicts the model and will be referred to throughout this section.

3.2.1 Stage 1: Realisation

An AdvEvent-related trauma occurs initially at the individual level. This might be a result of their own actions in enabling the AdvEvent (Stage 1 in Fig. 4), constituting the origin event (Maitlis and Christianson, 2014), distinct and disruptive to the individual, punctuating their routine activities (Trauma1). The AdvEvent might have arisen though misplaced trust in the effectiveness of the organisation's security systems, or being duped as to the intentions of a third party, or a failure to verify the source of an email. If the AdEvent occurred due to social engineering, the enabling insider is a victim of a trust violation in terms of their relationship with an unknown party and also, albeit unintentionally, the perpetrator of a trust violation in their relationship with their employer. Indeed, cybercrime may be the only misdemeanour where the victim shares some of the fault [Redacted].

This dual role creates an unexpected rise in vulnerability for the individual. Their initial reaction is likely to be shock, with further jolts as they comprehend the reality of an AdvEvent and what it might mean for them, their employer, and their relationships within the organisation.

Given the unexpectedness of the AdvEvent, negative emotions are likely to dominate (Kiefer, 2005). These are the first cue in sense-making related to the event and its transformation into an anchoring event (Ballinger and Rockmann, 2010). Prior study of emotion has tended to focus on a single or similarly-valenced emotions (Kiefer, 2005), but recent examination of AdvEvents shows that individuals experience divergent, concurrent and multiple negative emotions (Renaud et al., 2022), which constitute psychological harm (Agrafiotis et al., 2018). Typical are: anger, a fight response arising from their sense of betrayal; anxiety, a flight response in the face of what might have been lost and the realisation of what could follow; and shame, a specific flight response where the event is attributed to the individual personal deficiencies [Redacted]. The trust literature suggests that individuals who feel trusted by their employers might experience a sense of responsibility to repay and live up to felt trust (Baer et al., 2015). Hence, the emotions experienced at this stage are at a relatively individual level, and are triggered by the social environment of their organisation and existing relationships with key organisational stakeholders.

Prior organisational messaging around cybersecurity will frame individual understanding of the ramifications of their actions. SIP theory indicates that peers' experiences of how colleagues utilise cybersecurity training in shaping their behaviours will inform their reactions (Searle and Rice, 2024). Unfortunately, cybersecurity training and practices are dominated by fear and shame appeals designed to ensure compliance (Renaud and Dupuis, 2019)[Redacted]. This might prime the individual to hide because they fear that others will see the consequences of their assumedly deficient moral character (Greenbaum et al., 2020).

Although the social environment might shape the kind of emotion that the enabling insider experiences in response to trauma, that emotion itself also exerts an influence that shapes cognitions about the event and informs decision-making about appropriate next steps. For example, shame and guilt are emotions with high levels of certainty and a sense that the blame for what has occurred is attributable to things under the individual's control (Lerner et al., 2015). Individuals experiencing these emotions following the shock of an AdvEvent realisation are more likely to attribute blame to themselves, and to expect that others might do the same. In these cases, the enabling insider might try to hide the AdvEvent (Broomfield, 2019). In contrast, feelings of anxiety or fear introduce uncertainty and a sense that the negative event was attributable to situational factors (Lerner et al., 2015). In these cases, the individual might feel more confident about raising concerns.

The enabling insider's realisation and initial sense-making following the AdvEvent and specifically their role in it is a critical anchoring event in their relationship with their organisation. It is characterised by unfolding uncertainty and the growing realisation of their own vulnerability, and through them, that of the wider organisation (Fig. 3). Early emotional experiences have a crucial impact in shaping subsequent sense-making as they inform cognitive processing, skewing which memories are accessible and subsequent decision-making (Forgas, 2008; Fugate et al., 2011).

These cognitive biases constrain cognitive processing, bounding the availability and intuitive thinking that reduces the individual's available resources to process the event (Kahneman, 2003). Many cyber attackers deliberately exploit exactly these framing effects to diminish detection of their nefarious activities (Hassandoust et al., 2020). The profusion of negative emotions also influences subsequent sense-making about the individual's relationship with other organisational stakeholders (Ballinger and Rockmann, 2010) and biases decision-making about the risks inherent in next steps (Gigerenzer, 2004).

While the individual might think that they are able to control when and how to divulge details about the event to organisational stakeholders. In reality, their emotional reactions can lead others around them to become aware that something has occurred (Salancik and Pfeffer, 1978). SIP theory contends these emotional experiences and sense-making drawn from previous events are likely to shape the decision whether to report this event, as well as its timing, recipients and information divulged (van de Weijer et al., 2021). The waves of emotion that accompany early internal or external attributions of blame, and perceptions of how others might react given past experiences and current levels of trust, can create further confusion, making coherent reporting challenging (Van der Kolk, 2014). The resulting incoherence can have negative future implications for others' attributional processes (Stage 2 in Fig. 4).

3.2.2 Stage 2: Reveal

During this stage, the occurrence is revealed, requiring a choice of path to be made (Fig. 4). The second stage marks the transition of the experience beyond the enabling individual to other organisational actors. In some instances, individuals might choose to report, or to stay silent. In the latter case, others' could be exposed via other sources (Buckley et al., 2023). It is important to note the significance of context, specifically social, relational and situational, all affecting perceptions of vulnerability (Salancik and Pfeffer, 1978). Context includes prior organisational trust levels, trustworthiness and the fairness of prior social and organisational relations (Barclay and Kiefer, 2019; Gustafsson et al., 2020) (Figs. 2 and 3).

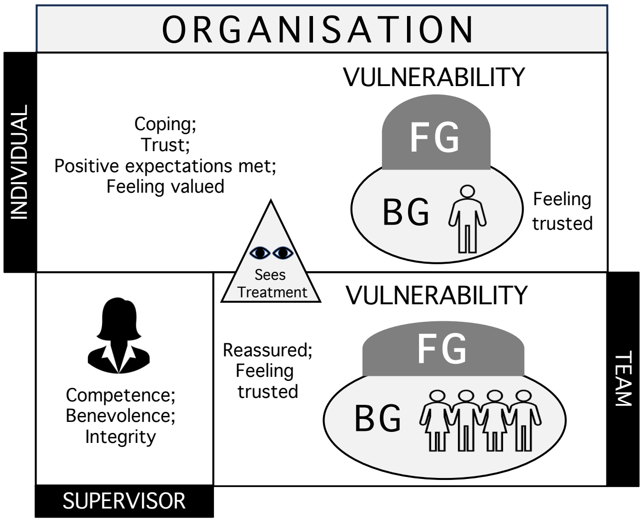

Figure 2: Increasing Trust when Vulnerability is in the Background (FG=Foreground; BG=Background)

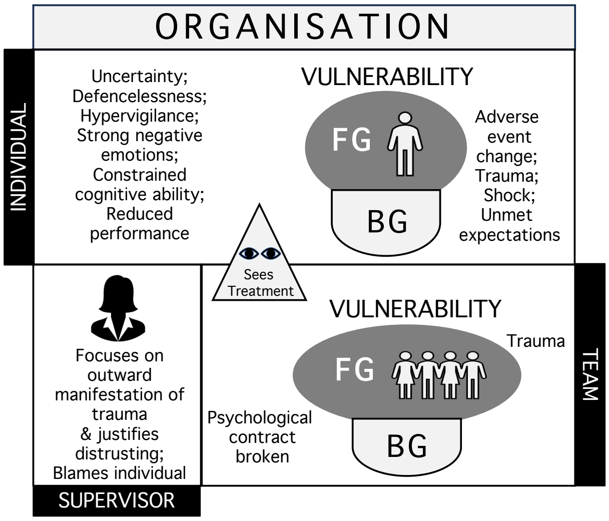

Figure 3: Decreasing Trust when Vulnerability is Foregrounded (FG=Foreground; BG=Background

Others' assessments of events are likely to informed by two kinds of information provision asymmetry – (1) prior knowledge about the individual (interpersonal), and (2) incomplete knowledge about the AdvEvent. That said, the stakeholder the enabling individual chooses to disclose to will likely have access to more complete information, and often more direct knowledge of the individual than those in later stages. Their reactions and the emotions they display are informed by this information. Where they are less familiar with the individual, their own propensity to trust is likely also to inform and shape their perspectives and responses (Colquitt and Rodell, 2011). Ultimately, the trust context within the organisation influences 'whether', 'how', 'when', and to 'whom' the individual discloses the AdvEvent. These dimensions will influence subsequent responses.

These early responses and reactions creates a critical second wave of cues for the enabling individual as well as for peers and supervisor. This further shapes how they make sense of what has happened and their vulnerability in relation to the event. This stage also represents the first realisation or anchoring event (Ballinger and Rockmann, 2010) for other stakeholders (CW-Trauma1, S-Trauma1). The introduction of further referents and levels adds complexity and potential divergence to trust (Fulmer and Gelfand, 2012) and AdvEvent responses.

For supervisors, this stage can be characterised as having a bottom-up trajectory (Morgeson et al., 2015), with exposure to the breach event rising through the organisation's hierarchy. Trust can become a germane concern arising from the salient vulnerability to which they are now privy. This is especially the case when security staff have informed them of having triggered an event rather than the individual realising this.

Ultimately, experiences during this reveal stage reinforce a divergence in how AdvEvents influence trust across organisations. Early reactions and responses are likely to determine subsequent trajectories in dealing with the event and its consequences. We delineate two distinct paths, one focusing on blame attribution that amplifies and makes salient the vulnerability of the enabling individual (Fig. 3), or a second focusing on understanding the incident and supporting the enabling individual Fig. 2, which actually reduces the salience of their vulnerability and relieves discomfort.

Vulnerability-Amplifying Route: Supervisor Perspective

The transitions into Stage 2 (Fig. 4: upper section), includes the emotional state of the enabling individual becoming visible to others through nonverbal, verbal and paraverbal signals (Van Knippenberg, 2018). These are particularly salient to the REVEAL stage. The supervisor's role now requires them to make inferences and attributions about the AdvEvent, its source and the vulnerability created from what has been lost (Searle and Rice, 2021) as well as potential future consequences. Unfortunately, gaining insights from a shocked individual might provide incomplete insights and potential inaccuracies, as both are involved in intense emotion-infused sense-making (Van der Kolk, 2014).

During these early stages, the emotional signals of the enabling individual provide important cues to the supervisor (van Kleef, 2022). If the enabling individual discloses the event, the supervisor's own emotional reaction and understanding of the event will be shaped by this fact. Through a process of emotion contagion, individuals' expressions of self-condemnation, such as shame, can suggest a flawed moral character, while guilt shown by a remorseful individual indicates reflection into how their actions contributed to the AdvEvent (Greenbaum et al., 2020). In contrast, other-condemning affective responses, such as anger, can trigger unhelpful blame spirals, perceived as the individual's attempt to shift the blame.

Emotional displays of the enabling individual are likely to influence supervisor's assessment of their trustworthiness, confirming or disconfirming initial perceptions of guilt through the provision of trust cues. Prior trustworthiness assessments may have some impact, informing the nature of subsequent information searches, and, critically, the capacity to entertain contrary views about the individual (White et al., 2003). If others have reported the event, trustwothiness is already in question. The jolt from an AdvEvent and this individual's reaction necessitates an active review of evidence regarding whether they can actually be trusted (Ashforth et al., 2008; Weibel et al., 2023). SIP theory (Salancik and Pfeffer, 1978) suggests how information will be filtered with recent events skewing others' assessment of the individual's trustworthiness, with greater lenience given to those who raise concerns and apologise than to those who deny or shift responsibility. Cybersecurity knowledge will also inform assessment of competence and integrity, as do existence of social norms where rules are ignored. Here, too, knowledge is likely to be asymmetric, with security staff having greater insight. Indications of the AdvEvent's severity, novelty and strength will be amplified by the associated negative valence, which can also increase the level of attention the individual is subjected to (Baumeister et al., 2001). Perceived trustworthiness of the individual will be significantly challenged if the report comes from another party, raising concerns about competence if they did **not** know, or their integrity if they are *choosing not to report.*

Cognitive biases, such as fundamental attribution error (Ross, 1977), are likely to focus the supervisor's attention onto the individual rather than influential situational factors. In the cyber context, concerns about threat severity and potential damage to the organisation's reputation add pressure for a speedy resolution that might mitigate further trust loss (Gillespie and Dietz, 2009). These pressures impoverish cognitive processes, as the supervisor begins their own Stage 1 realisation and sense-making (Trauma1). As a consequence, neither party is likely to be operating at full cognitive capability as they strive to make sense of the AdvEvent. Early causal attributions cause a bounding effect that can focus attention on the source (locus of causality), controllability and stability (Tomlinson and Mryer, 2009), with the level of negative experienced emotional intensity exacerbating bias (Forgas, 2008). Efforts to consider an external AdvEvent cause add complexity with misconceptions about its stability and controllability (Tomlinson and Mryer, 2009). Blaming the individual is appealing, as it offers the means to resolve things quickly, and to reduce the salience of their own vulnerability.

However, as seductive as this is, premature conclusions leave the organisation at risk from the situational causatives (Stage 3, Fig. 4) (Kim et al., 2004). Evidence suggests that premature closures are not unusual with unfair blaming of individuals based on little, or no, confirmatory evidence (Turton and Mehrotra, 2021). Unfortunately, this response will exacerbate subsequent vulnerability.

Vulnerability-Amplifying Route: Enabling Individual Perspective

The vulnerability-amplifying route is characterised by strong negative supervisor emotions directed towards the enabling individual, such as anger or disgust. These emotional displays, and the communication that accompanies them, comprise the first social cue the enabling individual has that signals how their involvement in the event might be regarded in their organisational social network, and the extent to which their behaviour aligns with organisational expectations.

The perception of high-activation negative emotions provide two forms of critical information (Van Kleef, 2009). *First*, the supervisor's anger can trigger a process of emotion contagion influencing their own emotional state. This process can result in either the contagion of similar emotions (you are angry, and that makes me feel angry), or dissimilar emotions (you are angry, and that makes me feel afraid) (Van Kleef, 2014). *Second*, the display of high activation negative emotion provides cues as to the other's character and goodwill in dealing with this vulnerability-inducing situation. SIP theory suggests such information will influence subordinates (Salancik and Pfeffer, 1978). Significantly, supervisor benevolence and integrity are relevant to perceived vulnerability (Kim et al., 2023; van der Werff et al., 2023). Displays of anger or disgust are likely to prompt an evaluation of low benevolence and the perception that this supervisor is not concerned about their needs. Together, these paths enable the supervisor's emotional displays to shape emotional and cognitive experiences of the enabling individual.

Being blamed and scapegoated has direct implications (Renaud et al., 2021a) and creates a further shock (Trauma2). They realise that their trust in the supervisor (demonstrated through their disclosure) is misplaced (Deutsch, 1958). This will trigger further emotionally-fuelled sense-making, depleting their resources even further (Maitlis and Christianson, 2014). Questions about their integrity attack their character and identity, increasing their vulnerability, and also reducing the means to repair lost trust (Tomlinson and Mryer, 2009; Kim et al., 2004, 2006). The individual response may reject this tainting by requiring accusers to substantiate accusations (Hendry et al., 1989). This too can further distract them from their work, leading to imputations of reduced trustworthiness, and less ability to cope (Chambers, 1989).

The supervisor's vulnerability-amplifying response has significance for ongoing relations, at best reducing trust levels, but more probably shifting to distrust based on evidence of the harm they do to the individual (Bijlsma-Frankema et al., 2015). This second trauma exacerbates vulnerability due to the perceived injustice of the reaction (Barclay and Kiefer, 2019). These precipitate a downward spiral of events characterised by negative responses including flight, flight or freeze, reducing the enabling insider's means, but now also their willingness, to offer information about the AdvEvent (Barclay et al., 2005; Van der Kolk, 2014). The resulting information loss reduces perceived trustworthiness, and also subsequent consequences for the organisation (Barclay and Kiefer, 2019) (Stage 4, Fig. 4).

Vulnerability-Relieving Route: Supervisor Perspective

While this alternative pathway does not remove the sense of vulnerability, it is a powerful means of reducing the salience thereof for both the enabling individual and the supervisor, and subsequently for other employees. It demonstrates a willingness to preserve trust (Fig. 4: lower section). The supervisor's more compassionate response acknowledges uncertainty and more significantly reduces the level and magnitude of risk for the enabling individual (Barclay and Kiefer, 2019) (Fig. 4: lower section).

The supervisor's compassion and empathy are related to goodwill and concern for others (Michie and Gooty, 2005; Greenbaum et al., 2020). As in the vulnerability-amplifying pathway, the experience and display of these emotions will be influenced by the quality of the prior relationship with the enabling individual. By choosing this path, the supervisor's competence is conveyed which helps to reduce uncertainty and signals support for the enabling individual.

Extant study shows supervisors differ in their capacity for positive, other-directed emotions (Gooty et al., 2010; Michie and Gooty, 2005), yet these positive displays are vital for their effectiveness (Edelman and Van Knippenberg, 2017). In focusing on the incident rather than assigning blame, the supervisor's competence is confirmed (Lapidot et al., 2007), liberating him/her to gather information to improve understanding of the AdvEvent (Zimmermann and Renaud, 2019), enhancing the quality of two-way communication and preserving trust (Gustafsson et al., 2020). Focusing attention on events demonstrates fairness in the investigation process, boosts calm and defuses further uncertainty for all (Chambers, 1989). Such impartiality can be challenging if the enabling individual was previously untrusted, or was an atypical team member (Ashforth et al., 2008). However, magnanimity signals supervisor trustworthiness, critical to eliciting information, and influencing expected responses from others. These actions demonstrate the authenticity of their own and the organisation's values of integrity and respect for others, and engender trust (Weibel et al., 2016) (Fig. 4).

Crucially, to contain wider reverberations, vulnerability-relieving responses enable the supervisor and enabling individual to traverse rapidly through this reveal stage as they: (i) avoid escalating negative emotions; (ii) maintain the quality of cognitions and judgements, (iii) engender better decision-making; and (iv) improve social relationships and communication quality. By so doing, they explicitly preserve and potentially build trust and retain vulnerability as a background concern. This response is less costly for the organisation and the different actors in the diversion of their time and effort from day-to-day functions, mitigating or avoiding many potentially negative consequences outlined in the other trajectory. Although mapped in the same way as the first path, this path does not make vulnerability a salient concern for as many employees (Barclay and Kiefer, 2019) (Fig. 2). Where vulnerability *does* manifest, it is resolved quickly and has less impact. The possibility of creating subsequent anchoring events between other actors across the different levels dissipates.

Vulnerability-Relieving Route: Enabling Individual Perspective

This route makes for a very different affective and cognitive experience for the enabling individual. As before, the emotions displayed by the individual provide crucial social cues denoting how the organisation and the individual understand their role in dealing with the AdvEvent. A supervisor that responds with low activation positive emotions, such as calm and compassion, de-escalates the enabling individual's higher activation negative emotions experienced during Stage 1 through emotional contagion processes (e.g., you feel calm, so I feel calm) and by signalling their goodwill and trustworthiness. This compassionate and empathetic response demonstrates benevolence and integrity, which are crucial in alleviating vulnerability and preserving trust (Colquitt and Rodell, 2011; Gustafsson et al., 2020). The efficacy of empathetic leadership during AdvEvent aftermaths has been demonstrated in case study work that illustrates empathetic senior management interventions as supporting a reduction in negative emotions (Stacey et al., 2021).

The individual's response to the supervisor is likely to be one of relief and reduced anxiety (Barclay et al., 2005) (Fig. 2). Their trust in the supervisor is preserved, with ambiguous actions interpreted positively (Deutsch, 1958). Their retained self-efficacy and confidence (Lau et al., 2014) can lead to subsequent job performance improvements (Stage 4). They may even have a sense of gratitude (Ritzenhöfer et al., 2017) in having been able to embrace the opportunity to master this threat (Stage 3). These positive emotions can trigger reciprocal increases in the level of supervisor trust with potential subsequent benefits to the wider organisation (Fehr et al., 2017).

Through this de-escalation process, the supervisor supports the enabling individual, avoiding triggering further trauma and facilitating a clearer recall of AdvEvent details (Van der Kolk, 2014). They remain willing to share further information (Nerstad et al., 2018), and their positive emotions are associated with ability and engagement (Watson et al., 1999; Barclay and Kiefer, 2019) (Fig. 2). Fredrickson et al. (2003) argue that experiences of gratitude, love, and other positive emotions enhance psychological capacities and increase resources to deal with serious, negative events. Together, the supervisor's early reactions to learning about the AdvEvent have powerful ramifications both for the disclosing individual's emotional and cognitive functioning, and the organisation's capabilities in responding and dealing with the AdvEvent.

3.2.3 Stage 3: Reaction

As the organisation moves beyond the initial realisation and reveal stages, awareness of the event and early responses will ripple out to other organisational stakeholders: i.e., co-workers and management. The prior choices of vulnerability-amplifying or relieving pathways are extended, denoting a shift in the spatial dispersion of the origin event with reactions that have their own strengths (Morgeson et al., 2015). AdvEvents are likely to have top-down and/or bottom-up moderating effects with reactions having implications beyond the relationship with the enabling individual. These spatial dispersions occur from both the high affective characteristic of reactions (van Kleef, 2022), and their social information significance (Salancik and Pfeffer, 1978) as knowledge spreads of the event and responses.

The initial awareness of the wider team is likely to be a more information-laden realisation than that experienced by the enabling individual. News of the AdvEvent comes alongside social information about whether and how the individual responded and reported the event as well as how the supervisor (or other) responded (Salancik and Pfeffer, 1978). However partial the information, it provides cues to understanding the event and personal vulnerability in relation to it. The more widespread salience of vulnerability makes trust a germane *foci* and sense-making regarding trust in the supervisor and, through this, the wider organisation. While the first stages set the organisation on the path of amplifying or relieving vulnerability, the organisation is now propelled into a self-reinforcing spiral (Nurse et al., 2014). We consider, first, the vulnerability-amplifying route.

Vulnerability-Amplifying Route: Enabling Individual Perspective

This path builds from prior stages, notably reactions of those who received the initial information, with the potential for traumas to extend to the team (Fig. 4: upper level Trauma3). This stage is characterised by further erosion of trust in the supervisor and organisation, as a consequence of increased vulnerability. An important and paradoxical additional characteristic of this stage stems from asymmetric information provisions of further social actors. This scrutiny of, and judgement about, the enabling insider's actions and intentions propel them and the organisation into crisis (Nurse et al., 2014). The piecemeal information diffuses across the local environment and creates further anchoring events between the individual and co-workers (Ballinger and Rockmann, 2010) (Fig. 4: Trauma3, CW-Trauma1).

Subsequent anchoring events further disrupt the local environment with negative emotion and sense-making, depleting cognitive capacities, and critically reducing resources for cybersecurity activities (Maitlis and Christianson, 2014). Collectively, asymmetric awareness of the AdvEvent and impact undermines threat reduction efforts. Therefore, while the magnitude of threat from a external AdvEvent source remains and is intensified for the organisation through resultant destabilisation across multiple organisational relationships. The supervisor, in withdrawing trust from the enabling individual, damages their self-image, and undermines their social standing (Skinner et al., 2014). When similar negative reactions occur from co-workers, the individual's vulnerability increases. The further negative spiral instigated by the team consolidates their new out-group status (Ashforth et al., 2008). The shift in relations with multiple others denotes their more resolved position as 'distrusted' (Lewis and Weigert, 1985). As each co-worker reaches similar conclusions, further traumas arise for the enabling individual (Fig. 4: upper level, Trauma3), fuelling a now overwhelming sense of vulnerability, especially if co-workers were friends (Dirks and Ferrin, 2001).

Vulnerability-Amplifying Route: Co-Worker Perspective

The enabling individual's scapegoating by the supervisor and other key actors, is viewed as humiliation and victimisation (Renaud et al., 2021a; BBC, 2019). The paucity and partiality of the rapid search for a culprit and unjust treatment of the enabling individual cynically designed to confirm their 'witch-hood' make vulnerability a salient concern (Mathers, 2021; Wolff, 2018). This cynical scapegoating prevents greater understanding of the AdvEvent and underplays its complexity. Together, these failures demonstrate supervisor and other key actors' untrustworthiness i.e., incompetence, lack of integrity, and failure to care and respect for the individual.

The stage model spatially shifts, adding top-down and/or bottom-up moderated events that denote the emergence of a third wave of salient vulnerabilities, with potentially eroded trust now extending to the team (Lapidot et al., 2007). A myopic focus on a convenient internal threat means the technical systems that enabled the AdvEvent remain unpatched, with the failure to appreciate alternative situational factors increasing overall risk (Rice and Searle, 2022).

SIP theory (Salancik and Pfeffer, 1978) contends that these events become important sources of social information. Employees manage their escalating uncertainty through their own active searches for trusted information. These reactions denote the opening of further event spaces, changing the spread and spatial direction with top-down reactions moderating novel horizontal reactions (Morgeson et al., 2015). These developments reflect growing vulnerability arising from a relative lack of power, dependence on key actors and increasing sense of vulnerability (Vanneste et al., 2014). Escalating knowledge of the origin event produces anchoring events, (Fig. 4: CW-Traumas). These breaches of trust (Kim et al., 2004) include negative emotions of anxiety or anger at unjust treatment (Greenbaum et al., 2020), triggering widespread sense-making with the supervisor's response denoting the social effects of emotions (van Kleef, 2022).

These processes are multi-level, affecting Co-Worker relational dynamics, both with the supervisor and each other, leading to further anchoring events in these relationships. Uncertainty becomes contagious with rising vulnerability and limited formal information leading to proliferation of hyper-vigilance with employees questioning key actors' actions and intentions (Gustafsson et al., 2020). Critically for the organisation, such proliferation diverts attention and reduces self-regulation (Baumeister et al., 2001), increasing the risk of future AdvEvents. Previous work demonstrates the importance of collective cybersecurity self-efficacy which is critical in shaping effective security related behaviours (Yoo et al., 2020).

Within the team, specific attention focuses on the supervisor (Whitener et al., 1998) with trust threatened by divergence between their words and deeds (Simons et al., 2015). Observing a leader's unjust and disrespectful actions can be vulnerability inducing, adding important social information (Salancik and Pfeffer, 1978). Concerns about unjust processes are associated with negative emotions of anxiety and anger (Barclay and Kiefer, 2019). These accelerate trust reduction, especially amongst those who identify with the enabling individual (Rice and Searle, 2022). Each disconnect has the potential to add to the event space, with strong negative emotions and further sense-making characterising the reviewing of prior trust decisions (Kim et al., 2004).

There can be a dynamic magnitude and speed of change to the active processing of trust (Baer et al., 2015). A spiral of hyper-vigilance and vulnerability can become self-fulfilling, triggering reviews of previously-resolved trust decisions across multiple referents, each accompanied by further negative emotions and cognitive overload that reduce the quality of these cognitions and judgements (Forgas, 2008). As a result, many individuals experience anchoring events as relations decline with emotion-induced sense-making demands further diverting attention on the original event (Ballinger and Rockmann, 2010). The escalating sense of vulnerability can alter observers' prior decisions to remain with the organisation (Spreitzer and Mishra, 2002).

The unfolding crisis is characterised by information gathering due to the often untimely, inadequate, incomplete or inaccurate organisational internal communications during crises (Rice and Searle, 2022). This can further reduce trust, with attention shifting to the team for cues and signals to resolve rising uncertainty (Salancik and Pfeffer, 1978). These new searches centre on prototypical members (Ashforth et al., 2008), whose actions set the response tone, indicating the required actions and reactions (Barreto and Hogg, 2017). The transition into a state of vigilance (Gustafsson et al., 2020) creates opportunities for further misunderstandings.

High levels of scrutiny can cause previously insignificant relationship matters between team members to become noteworthy, triggered by subtle emotional exchanges between actors (Van Knippenberg, 2018), or perceived signals of declining trust in relationships (Lau et al., 2014). Social information from networks of more trusted people become increasingly significant as employees try to navigate their own way through dynamically-shifting events (Searle and Rice, 2024). These have further negative consequences for trust across the organisation. Supervisors' reactions to the now-distrusted enabling individual necessitates their work be re-allocated to trusted team members, opening up fresh event spaces, based on the perceived fairness/unfairness of these allocation decisions (Barclay and Kiefer, 2019), triggerring scrutiny of supervisors' trustworthiness (Colquitt and Rodell, 2011; Bijlsma-Frankema et al., 2015).

These events have greater significance to the team when a trusted person is assigned re-allocated tasks (Salancik and Pfeffer, 1978) adding to their workload (Baer et al., 2015), risking overwhelming them and escalating risk further AdvEvents. Subtle emotional signals offer cues for the wider team denoting changing relations between these trusted employees and their supervisor, adding fresh vulnerabilities (van Kleef, 2022).

Vulnerability-Relieving Route

The supervisor's prior actions, focusing on the event rather than the enabling individual, have made this a relatively diminished event space with muted short-lived horizontal reactions from the team making this a non-event. The reduced emotional intensity de-escalates the means for social emotional contagion (van Kleef, 2022) and the need for SIP (Salancik and Pfeffer, 1978).

Vulnerability-Relieving Route: Enabling Individual Perspective The procedural and informational justice in the treatment of the enabling individual provides important trustworthy signals about the supervisor and other key organisational actors (Colquitt and Rodell, 2011), especially their openness of communication and demonstrations of care and respect (Korsgaard et al., 2002). These reduce the salience of vulnerability from internal sources. Actions are noted by Co-Workers (Salancik and Pfeffer, 1978) with the individual's social standing remaining intact. avoiding further traumas. These experiences may add to the individual's feelings of relief, gratitude and even elation in response (Greenbaum et al., 2020). As a result, their well-being improves, increasing prosocial responses. Indeed, these reactions may help the individual recover memories about the

AdvEvent that augment the organisation's information and understanding. These improved social exchanges denote improved trust (Colquitt and Rodell, 2011). Feeling trust despite the AdvEvent can lead to a positive trust spiral boosting productivity and prosocial behaviours (Searle, 2018).

Vulnerability-Relieving Route: Team Perspective

The supervisor has provided social information cues about how colleagues should treat the enabling individual (Salancik and Pfeffer, 1978). Their modelling of compassion and a supportive response ameliorates trust erosion at other levels (Lapidot et al., 2007). Emotion-led contagion of vulnerability is avoided in the team (van Kleef, 2022) with the motivation to maintain trust confirmed by signalling value congruence and efforts to maintain relationships, even if costly in time (Gustafsson et al., 2020; van der Werff et al., 2019; Weibel et al., 2016). The dividends of such efforts are realised at this stage as team members perceive the trustworthiness of the supervisor with ramifications for their own willingness to be vulnerable in the organisation. As a result, vulnerability remains a background concern (Fig. 2). The enabling individual's and team's resolving of vulnerability confirms their existing views (White et al., 2003), maintaining, if not boosting, trust in the supervisor and the organisation. Given the limitations of cognitive resources, reduced vulnerability diminishes a source of demand and strain for employees (Lazarus and Folkman, 1984). This frees them to focus on their work, detecting and resisting future AdvEvents. The positive reaction of the supervisor increases the willingness of others to also come forward and share their AdvEvent experiences, providing the organisation with important information.

3.2.4 Stage 4: Restabilisation

This final stage is the culmination of the pathway choices. In the vulnerability-amplifying route, the failing of those in key roles, and organisational policies, to control cyber-threat have demonstrated the organisation's untrustworthiness and inability to respond effectively (Weibel et al., 2016) (Fig. 4). As a consequence, trust is eroded at different levels and often replaced by distrust making the situation more difficult to repair (Gustafsson et al., 2020). Hence, the potential vulnerability from external cyber attackers grows in significance, as the limitations of the cybersecurity policy, their own supervisors and senior leaders becomes evident. As such, the organisation has been rendered less resilient and resistant to current and future AdvEvents. This outcome is aptly demonstrated in the Sony case with loss of the CEO, key staff quitting and class actions being filed (Agrafiotis et al., 2018). In contrast, the vulnerability-relieving pathway has demonstrated the trustworthiness of the organisation's key actors and processes, and efforts to preserve trust (Gustafsson et al., 2020) making it more resilient and confident in its capacity to detect subsequent AdvEvents as employees are now more willing to share real-time cybersecurity concerns.

Vulnerability-Amplifying Route: Enabling Individual Perspective

The task of restoring trust damaged across multiple levels requires considerable and consistent action (Kim et al., 2004) yet there is little remaining energy for this now herculean task. In response, the enabling insider becomes increasingly withdrawn and isolated, making any effort they show more likely to go unnoticed, or, even worse, mis-attributed as further evidence of guilt (Dirks and Ferrin, 2001). Sadly for the organisation, the resulting ostracism reduces their means of being heard, even when raising genuine concerns (Jahanzeb and Newell, 2020). From an event space perspective (Morgeson et al., 2015), the organisation's cumulative actions have throttled important sources of information about the AdvEvent.

Feeling distrusted fuels a sense of internal dislocation (Chambers, 1989). The toxic combination of recurring negative emotions disconnects the enabling individual from others (Kiefer and Barclay, 2012). The experience of being distrusted has consequences for their self-esteem, leading to a reduction in performance (Lau et al., 2014). Moreover, hyper-vigilance from others makes this decline obvious, and provides further confirmation of their untrustworthiness. There is little recognition that this arose from mistreatment, rather than any underlying malfeasance. Any performance decline can also trigger attitude shifts from their remaining supporters leaving them further isolated. These multiple injustices increase anger and anxiety, further constraining their action options (Barclay and Kiefer, 2019).

The enabling individual's choices have important consequences for the organisation. Reactions to escalating victimisation can include: flight, which increases the risks of subsequent insider threat even after they have left the organisation (Nurse et al., 2014); an exit forged in anger makes retaliation seem a viable option (Skarlicki et al., 2008); or freezing, which has implications for effective job performance, necessitating others taking on their duties, and, in so doing, increasing vulnerability to subsequent AdvEvents. Performance management processes might be followed with potential for exit from the organisation (Weibel et al., 2016). This latter event has the potential to escalate vulnerability and diminish trust even further, driving perceptions of victimisation for others to see.

Vulnerability-Amplifying Route: Team Perspective

The treatment of team members who provided information about the initial AdvEvent informs general willingness to share further insights. As key actors have scapegoated the enabling insider, others may now be reluctant to provide information (Rice and Searle, 2022). These reactions discourage subsequent communication and shut down contrary information paths leaving supervisors with less insight about what is actually occurring and rendering them and the organisation still unclear about what has really happened. Experiences of the enabling insider reduce the willingness of other insider targets to come forward. Thus, team and organisational cyber-threat levels increase. Furthermore, the downward spirals of trust affect both levels, critically eroding the means of repair (Gillespie and Dietz, 2009; Lapidot et al., 2007). The Sony case class actions confirm this distrusting consequence (Agrafiotis et al., 2018).

In summary, this path reduces the information available within the organisation and the relational turbulence damages individuals' capacity for cybersecurity and more general self-regulation. Trust is damaged at multiple levels, often being replaced by distrust rendering an organisation less resilient with diminished capacity to detect and cope with cyber risks.

Vulnerability-Relieving Route

As noted earlier, the events and the positive reactions of key organisational stakeholders have provided evidence of the organisation's competence in handling AdvEvent information effectively and in preserving trust (Gustafsson et al., 2020). The multi-level reinforcement of this as a trustworthy organisation allows vulnerability to remain a background concern (Fig. 3). This frees up emotional and cognitive resources to remain focused on work, including the detecting and sharing of future AdvEvent information. These pro-organisational efforts make the organisation far more resilient to future AdvEvents.

In Conclusion

Having fleshed out the nature of each of the aftermath stages, we depict them in Fig. 4 with the differing time lines in Fig. 5. The next Section discusses the theoretical and practical implications of this model, the limitations and future research to be carried out.

4 Discussion

AdvEvents are common organisational events for which the financial and security implications are well established (Rosati et al., 2019). Despite the growing frequency of these events, there is an increasing awareness that we have yet to fully explore the wider social consequences of AdvEvents and in particular how they impact perceived vulnerability and trust processes for internal stakeholders directly involved in the incident and those who witness the event and organisational response.

In this paper, we developed a stage model theory (Fig. 4) regarding the social ramifications of AdvEvents. Using a trust lens, we reframed AdvEvents as an anchoring events that can trigger a progression through stages in which vulnerability becomes a salient concern with reducing trust potentially rippling through the organisation. We argue that early reactions and responses to the AdvEvent create two self-reinforcing cycles that either relieve, or amplify vulnerability for organisational stakeholders and influence both the organisation's capacity to manage the AdvEvent and the longer-term social fabric of the organisation.

4.1 Theoretical Contributions

Our paper makes four important contributions to the literature.

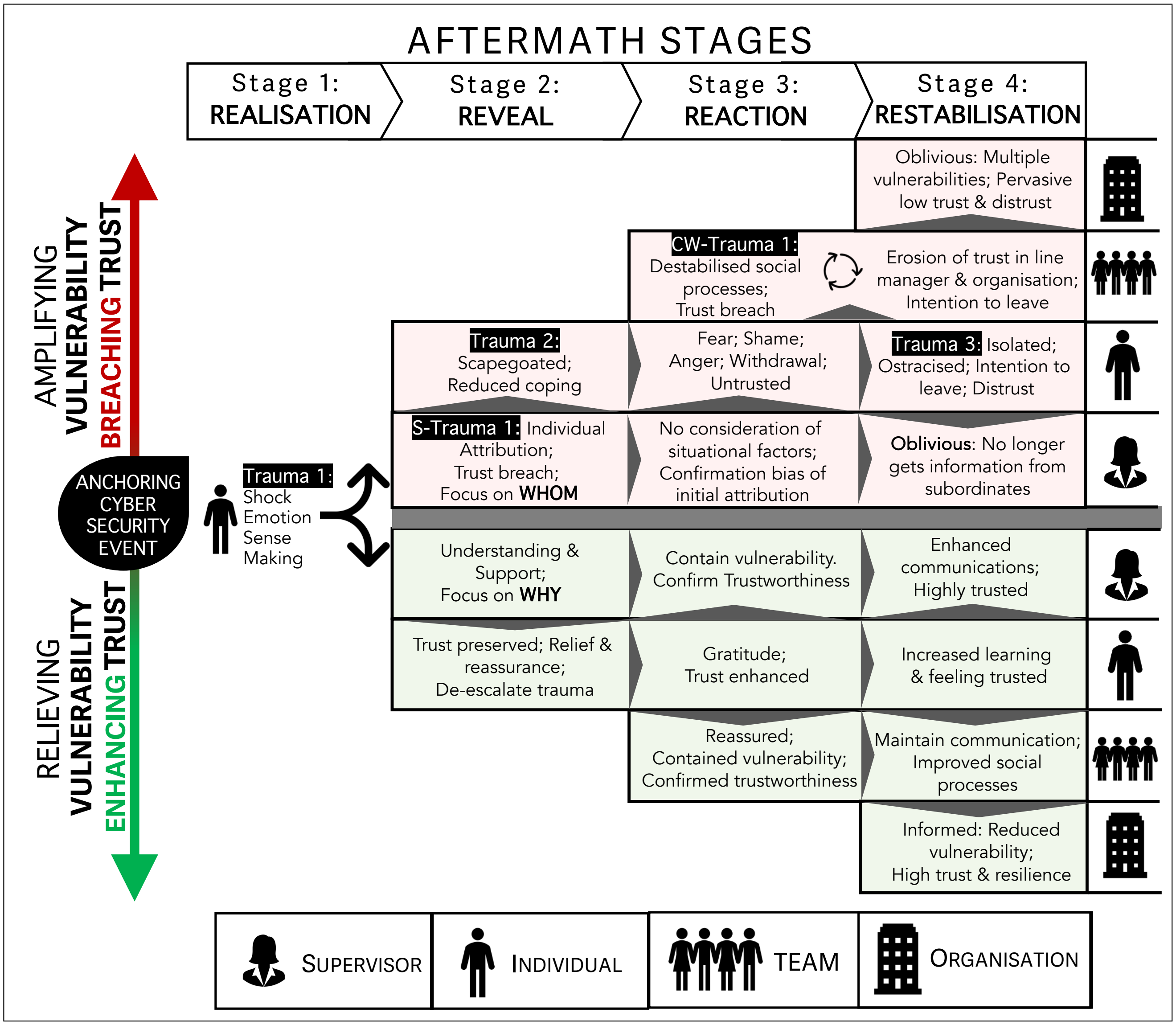
AFTERMATH STAGES
Stage 1: REALISATION
Stage 2: REVEAL
Stage 3: REACTION
Stage 4: RESTABILISATION
AMPLIFYING VULNERABILITY BREACHING TRUST
RELIEVING VULNERABILITY ENHANCING TRUST
ANCHORING CYBER SECURITY EVENT
Trauma 1: Shock Emotion Sense Making
Oblivious: Multiple vulnerabilities; Pervasive low trust & distrust
CW-Trauma 1: Destabilised social processes; Trust breach
Erosion of trust in line manager & organisation; Intention to leave
Trauma 2: Scapegoated; Reduced coping
Fear; Shame; Anger; Withdrawal; Untrusted
Trauma 3: Isolated; Ostracised; Intention to leave; Distrust
S-Trauma 1: Individual Attribution; Trust breach; Focus on WHOM
No consideration of situational factors; Confirmation bias of initial attribution
Oblivious: No longer gets information from subordinates
Understanding & Support; Focus on WHY
Contain vulnerability. Confirm Trustworthiness
Enhanced communications; Highly trusted
Trust preserved; Relief & reassurance; De-escalate trauma
Gratitude; Trust enhanced
Increased learning & feeling trusted
Reassured; Contained vulnerability; Confirmed trustworthiness
Maintain communication; Improved social processes
Informed: Reduced vulnerability; High trust & resilience
SUPERVISOR
INDIVIDUAL
TEAM
ORGANISATION

Figure 4: Social Information Processing Stage Theory Cybersecurity Event (CW=CoWorker; S=Supervisor)

First, we contribute to the cybersecurity literature using trust as a lens through which to examine and advance understanding of the social ramifications of AdvEvents. In doing so, we aim to expand discussion of how organisations can cope with AdvEvents to include insights from the organisational and social sciences. As well as preventing AdvEvents and reducing their attack surface, organisations should better prepare leaders, at all levels, to respond to AdvEvents when they occur.

Second, we make three contributions to expanding our understanding of trust by focusing on context in which uncertainty abounds, namely an AdvEvent. Specifically, in the context of high levels of uncertainty we consider organisational event sequences to develop new theory regarding the dynamics and trajectories of trust and the formation of self-reinforcing trust spirals (Korsgaard et al., 2018).

Third, our integration of SIP theories (Salancik and Pfeffer, 1978; Van Kleef, 2009) builds on previous work

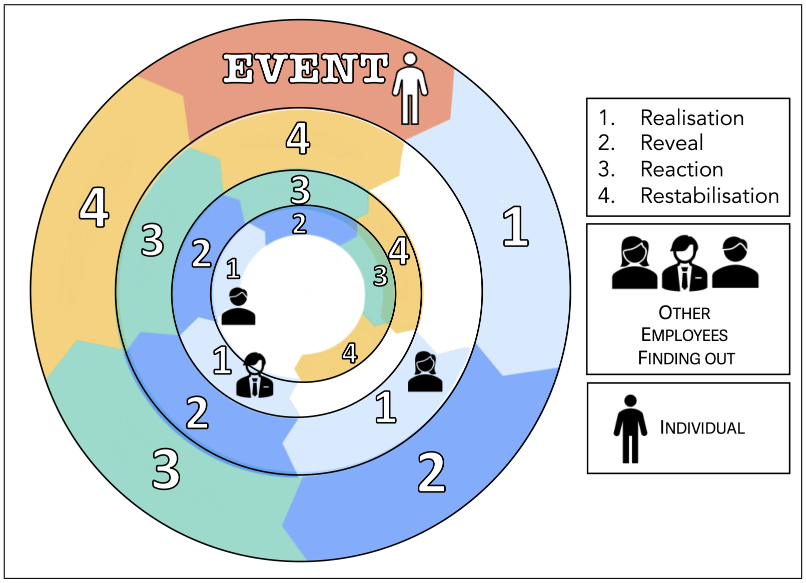

Figure 5: The 4 stages start over each time someone new finds out about the security incident. In the diagram: spirals reflecting the repeating nature of this phenomenon until all employees become aware

on the antecedents or bases of trust (Mayer et al., 1995; McAllister, 1995) by expanding the discussion beyond a relatively passive reaction to trustworthiness to consider how signals from the wider relational environment and the trustee can shape both trust itself and how we search for cues to inform trust (Dietz, 2011).

Fourth, we draw on theories of emotion as social information (Van Kleef, 2009), to answer calls from recent reviews of the literature (Legood et al., 2023; Lee et al., 2023) to develop theory on the role of emotion and emotional displays in building trust within organisations. Our model moves emotion to the centre stage of trust by arguing that the emotional displays of key stakeholders in the organisation provide critical cues for individuals striving to understand organisation-level events and how these might impact their own vulnerability and trust.

4.2 Practical Implications

Our research delineates vulnerabilities in an organisation as an important consideration in informing actions in the aftermath of AdvEvents. Through identifying four distinct stages for these events, we reveal important transition points around which awareness and support can be focused. Specifically, we outline the critical role of the supervisor and initial recipients of the enabling insider's concerns and their dynamics. There is value to raising awareness of the subtle emotional clues that an AdvEvent has occurred, and in how their own emotional reactions send signals to set the tone and constrain the scope of their own and others' cognitive processes. We show merit of training that promotes awareness about emotional reactions, and also more open enquiry that advances understanding of what has occurred and why, rather than simply attributing blame. Providing guidance to support the enabling insider's clear recall of events has dividends for them and the organisation.

Similarly, improving the skills that engender active trust preservation results in wider benefits for them as a key organisational actor, and from modelling how others should be treated demonstrating their own trustworthiness (Gustafsson et al., 2020). These are important skills for leaders to avoid the contagion of negative emotions, and the escalation of crisis through amplifying vulnerabilities across multiple observers. Further, such actions help ameliorate the potential of further distracting anchoring events as the event space disperses within the organisation. These activities help the emergence and maintenance of trust cultures through focusing on people as fallible but not necessarily malicious actors in these AdvEvents.

4.3 Limitations and Future Research

Our theorising in this paper discusses the intrapersonal and interpersonal impact of a AdvEvent through the lens of trust and vulnerability. The trajectories we set out illustrate the best and worst possible scenarios arising from an AdvEvent and our theorising should be interpreted in light of several limitations. First, while our theorising is based firmly in empirical evidence much of this evidence has been cross-sectional and focused on identifying nomothetic principles of human behaviour in relation to cybersecurity Cram et al. (2024). The arguments we develop in this conceptual paper will need to be investigated by future empirical research. In particular, through adopting the perspective of trust dynamics and their distinct trajectories, a number of future research opportunities emerge. First, this paper provides the conceptual framework for empirical study of the internal, organisational aftermaths of AdvEvents, identifying distinct levels for fruitful study, including individual differences in the trust violation cues (Bansal and Warkentin, 2021), and of the dynamics of dyadic individual-supervisor relations (Nienaber et al., 2015), as well as their spillovers and dynamics at the team level (Korsgaard and Bliese, 2021). While this focus was useful in maintaining theoretical parsimony, future work might consider extending our theorising by exploring the interaction of wider macro-organisational elements, such as cultural and values, and also communication policies to disrupt these trajectories would be important to understand the means of insulating organisations (Weibel et al., 2023; Rice and Searle, 2022). What, in particular, are the conditions in which these trajectories can be disrupted or stopped?

Our theorising is also limited by our focus on a particular type of cybersecurity event. Further study could also extend to exploring other events (cyber-related or otherwise) in which vulnerabilities become germane, and where choice of response is crucial specifically for those with heightened negative emotional tone and motivation to sense-make (van der Werff et al., 2019). For instance, prior study has included trust in websites following a data breach (Bansal and Warkentin, 2021). In organisational studies, events of particular interest to trust might include internal breach events, such as changes to psychological contracts, or betrayal, or more exogenous crises. Are there organisations or sectors that are particularly good at managing these crisis (e.g., emergency response organisations) or sectors with divergent outcomes with some having more events, and others have fewer? Important lessons can be learnt from comparative studies.

Finally, further research could be undertaken on emotion displays as a social cue and their role in conscious (or subconscious) information search when making trusting decisions. The study of emotions in the trust literature is a relatively neglected and yet growing topic of interest (Legood et al., 2023). A better understanding of trust and emotion has particular ramifications regarding how we understand vulnerability, and is likely to be closely entwined with questions of employee identification and dependency (Weibel et al., 2023). In the cybersecurity context, the extension of theory to include a better understanding of emotion has been valuable in improving understanding of how we can encourage security related behaviours (Renaud et al., 2021b). We call on researchers to consider the role of emotion in dealing with AdvEvent aftermaths.

5 Conclusion

Organisations face an increasing threat from cyber criminals seeking to exploit technical and human vulnerabilities. In this uncertain landscape, we argue that organisations need to focus their attention on how to prepare their leaders and employees to respond effectively to AdvEvents. We develop a stage-based SIP theory of how responses to AdvEvents can amplify or relieve vulnerability for key organisational stakeholders. While the vulnerability-amplifying route creates a negative reinforcing spiral that reduces trust for an increasing number of employees, the vulnerability-relieving route allows organisations to respond more effectively by using the AdvEvent to reinforce trust within their organisation.

References

Ioannis Agrafiotis, Jason RC Nurse, Michael Goldsmith, Sadie Creese, and David Upton. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1):tyy006, 2018. https://doi.org/10.1093/cybsec/tyy006.

Meryem Ammi, Oluwasegun Adedugbe, Fahad Mohamed Alharby, and Elhadj Benkhelifa. Taxonomical challenges for cyber incident response threat intelligence: a review. *International Journal of Cloud Applications and Computing (IJCAC)*, 12(1):1–14, 2022.

Anonymous. Accidental data breach by a trainee: consequences?, 2021. https://www.accountingweb.co.uk/any-answers/accidental-data-breach-by-a-trainee-consequences.

Charles Arthur. *Cyber Wars*. Kogan Page Ltd, 2018.

Blake E Ashforth, Spencer H Harrison, and Kevin G Corley. Identification in organizations: An examination of four fundamental questions. *Journal of Management*, 34(3):325–374, 2008. https://doi.org/10.1177/0149206308316059.

Associated Press. Sony settles hacking lawsuit, to pay up to $8 million, 2015. https://www.latimes.com/business/la-fi-sony-hack-settlement-20151020-story.html.

Michael D Baer, Rashpal K Dhensa-Kahlon, Jason A Colquitt, Jessica B Rodell, Ryan Outlaw, and David M Long. Uneasy lies the head that bears the trust: The effects of feeling trusted on emotional exhaustion. *Academy of Management Journal*, 58(6):1637–1657, 2015. https://doi.org/10.5465/amj.2014.0246.

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

Gaurav Bansal and Merrill Warkentin. Do you still trust? the role of age, gender, and privacy concern on trust after insider data breaches. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 52(4):9–44, 2021. https://doi.org/10.1145/3508484.3508487.

Laurie J Barclay and Tina Kiefer. In the aftermath of unfair events: Understanding the differential effects of anxiety and anger. *Journal of Management*, 45(5):1802–1829, 2019. https://doi.org/10.1177/01492063177391.

Laurie J Barclay, Daniel P Skarlicki, and S Douglas Pugh. Exploring the role of emotions in injustice perceptions and retaliation. *Journal of Applied Psychology*, 90(4):629–643, 2005. https://doi.org/10.1037/0021-9010.90.4.629.

Nicolas B Barreto and Michael A Hogg. Evaluation of and support for group prototypical leaders: A meta-analysis of twenty years of empirical research. *Social Influence*, 12(1):41–55, 2017. https://doi.org/10.1080/15534510.2017.1316771.

Stephen Battaglio and Richard Verrier. Sony shake-up possible after hack, analysts say, 2014. https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-shakeup-fallout-employees-20141219-story.html.

Roy F Baumeister, Ellen Bratslavsky, Catrin Finkenauer, and Kathleen D Vohs. Bad is stronger than good. *Review of General Psychology*, 5(4):323–370, 2001. https://doi.org/10.1037//1089-2680.5.4.323.

BBC. Company sues worker who fell for email scam, 2019. https://www.bbc.co.uk/news/uk-scotland-glasgow-west-47135686.

BBC. University of Manchester hit by cyber attack, 2023. Retrieved 9 July 2023 from: https://www.bbc.co.uk/news/uk-england-manchester-65855002.

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

Broomfield. Webroot report: Nearly half of employees confess to clicking links in potential phishing emails at work, 2019. Retrieved 9 July 2023 from: https://www.webroot.com/ie/en/about/press-room/releases/employees-click-phishing-emails-atwork.

J Buckley, D Lottridge, JG Murphy, and PM Corballis. Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. *International Journal of Human-Computer Studies*, 172:102996, 2023. https://doi.org/10.1016/j.ijhcs.2023.102996.

R Chambers. Vulnerability, coping and policy. *IDS Bulletin-Institute of Development Studies*, 20(2):1–7, 1989.

Thomas Claburn. Grand theft auto 6 maker confirms source code, vids stolen in cyber-heist, 2022. Retrieved 9 July 2023 from: https://www.theregister.com/2022/09/19/grand_theft_auto_6_hacked/.

Jason A Colquitt and Jessica B Rodell. Justice, trust, and trustworthiness: A longitudinal analysis integrating three theoretical perspectives. *Academy of Management Journal*, 54(6):1183–1206, 2011. https://doi.org/10.5465/amj.2007.0572.

W Alec Cram, John D'Arcy, and Alexander Benlian. Time will tell: The case for an idiographic approach to behavioral cybersecurity research. *MIS Quarterly*, 48(1), 2024. 10.25300/MISQ/2023/17707.

Reeshad S Dalal, David J Howard, Rebecca J Bennett, Clay Posey, Stephen J Zaccaro, and Bradley J Brummel. Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology*, 37(1):1–29, 2022. https://doi.org/10.1007/s10869-021-09732-9.

Antonio R Damasio. Descartes' error and the future of human life. *Scientific American*, 271(4):144–144, 1994. https://doi.org/10.1038/scientificamerican1094-144.

Rob Davies. Capita cyber-attack: Uss pension fund members' details may have been stolen, 2023. Retrieved 9 July 2023 from: https://www.theguardian.com/business/2023/may/12/capita-cyber-attack-uss-pension-fund-members-details-may-have-been-stolen.

Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. Expert and non-expert attitudes towards (secure) instant messaging. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, pages 147–157, 2016.

Deloitte. 91 https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html.

Ben Densham. Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, 2015 (1):5–8, 2015. https://doi.org/10.1016/S1353-4858(15)70007-3.

M Deutsch. Trust and suspicion. *Journal of Conflict Resolution*, 2(4):265–279, 1958. https://doi.org/10.1177/002200275800200401.

Graham Dietz. Going back to the source: Why do people trust each other? *Journal of Trust Research*, 1(2): 215–222, 2011. https://doi.org/10.1080/21515581.2011.603514.

Kurt T Dirks and Donald L Ferrin. The role of trust in organizational settings. *Organization Science*, 12(4): 450–467, 2001. https://doi.org/10.1287/orsc.12.4.450.10640.

Kurt T Dirks, Roy J Lewicki, and Akbar Zaheer. Reparing relationships within and between organizations: building a conceptual foundation. *Academy of Management Review*, 34(1):68–84, 2009. https://doi.org/10.5465/amr.2009.35713285.

Peter J Edelman and Daan Van Knippenberg. Training leader emotion regulation and leadership effectiveness. *Journal of Business and Psychology*, 32:747–757, 2017. https://doi.org/10.1007/s10869-016-9471-8.

Ryan Faughnder. Sony Pictures CEO Michael Lynton to staff: Hackers 'won't take us down' , 2014. https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-meeting-pascal-lynton-20141215-story.html.

Ryan Faughnder. Tom rothman chosen as chairman of sony pictures' motion picture group, 2015. https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-tom-rothman-chairman-sony-pictures-20150224-story.html.

Federal Bureau of Investigation. Internet crime report 2020, 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (Accessed June 2023).

R Fehr, A Fulmer, E Awtrey, and J A Miller. The grateful workplace: A multilevel model of gratitude in organizations. *Academy of Management Review*, 42(2):361–381, 2017. https://doi.org/10.5465/amr.2014.0374.

J.P. Forgas. The role of affect in attitudes and attitude change. In WD Crano and R Prislin, editors, *Attitudes and Attitude Change*, page 131–158. Psychology Press, 2008.

Barbara L Fredrickson, Michele M Tugade, Christian E Waugh, and Gregory R Larkin. What good are positive emotions in crisis? A prospective study of resilience and emotions following the terrorist attacks on the United States on September 11th, 2001. *Journal of Personality and Social Psychology*, 84(2):365, 2003. https://doi.org/10.1037/0022-3514.84.2.365.

M Fugate, S Harrison, and AJ Kinicki. Thoughts and feelings about organizational change: A field test of appraisal theory. *Journal of Leadership & Organizational Studies*, 18(4):421–437, 2011. https://doi.org/10.1177/1548051811416510.

C Ashley Fulmer and Michele J Gelfand. At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management*, 38(4):1167–1230, 2012. https://doi.org/10.1177/0149206312439327.

Alexeis Garcia-Perez, Mark Paul Sallos, and Pattanapong Tiwasing. Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. *Journal of Intellectual Capital*, 24(2):465–486, 2023.

Caron E Gentry. Anxiety and the creation of the scapegoated other. *Critical Studies on Security*, 3(2):133–146, 2015. https://doi.org/10.1080/21624887.2015.1027600.

Gerd Gigerenzer. Fast and frugal heuristics: The tools of bounded rationality. *Blackwell Handbook of Judgment and Decision Making*, 62:88, 2004.

Nicole Gillespie and Graham Dietz. Trust repair after an organization-level failure. *Academy of Management Review*, 34(1):127–145, 2009. https://doi.org/10.5465/amr.2009.35713319.

Janaki Gooty, Shane Connelly, Jennifer Griffith, and Alka Gupta. Leadership, affect and emotions: A state of the science review. *The Leadership Quarterly*, 21(6):979–1004, 2010. https://doi.org/10.1016/j.leaqua.2010.10.005.

T Govier. An epistemology of trust. *International Journal of Moral Social Studies*, 8(2):155–174, 1994.

GOV.UK. Cyber security breaches survey 2022, 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.

R. Greenbaum, J. Bonner, T. Gray, and M. Mawritz. Moral emotions: A review and research agenda for management scholarship. *Journal of Organizational Behavior*, 41(2):95–114, 2020. https://doi.org/10.1002/job.2367.

Stefanie Gustafsson, Nicole Gillespie, Rosalind Searle, Veronica Hope Hailey, and Graham Dietz. Preserving organizational trust during disruption. *Organization Studies*, 42(9):1409–1433, 2020. https://doi.org/10.1177/0170840620912705.

Saba Hamedy and Ryan Faughnder. Timeline: After the hack: Sony pictures' road to recovery, 2015. https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-chronology-html-20141207-htmlstory.html.

Saba Hamedy and Meg James. Sony hit with lawsuit by former employees over email leaks, 2014. https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-class-action-lawsuit-employees-20141215-story.html.

Farkhondeh Hassandoust, Harminder Singh, and Jocelyn Williams. The role of contextualization in individuals' vulnerability to phishing attempts. *Australasian Journal of Information Systems*, 24, 2020. https://doi.org/10.3127/ajis.v24i0.2693.

Sarah H Hendry, David R Shaffer, and Dina Peacock. On testifying in one's own behalf: Interactive effects of evidential strength and defendant's testimonial demeanor on mock jurors' decisions. *Journal of Applied Psychology*, 74(4):539, 1989. https://doi.org/10.1037/0021-9010.74.4.539.

Amanda Hess. Inside the sony hack, 2015. https://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

Elizabeth Howlett. Two-fifths of firms have sacked staff for cybersecurity breaches during covid, poll shows, 2020. https://www.peoplemanagement.co.uk/article/1742894/two-fifths-firms-sacked-staff-cybersecurity-breaches-during-covid-poll-finds.

Sadia Jahanzeb and William Newell. Co-worker ostracism and promotive voice: a self-consistency motivation analysis. *Journal of Management & Organization*, pages 1–17, 2020. https://doi.org/10.1017/jmo.2020.22.

E Johns. Cyber security breaches survey 2020, 2020. Department for Digital, Culture, Media & Sport.

Jo Joyce. Into the breach – managing employees during a data incident, 2022. https://www.taylorwessing.com/en/global-data-hub/2022/july---managing-hr-data/into-the-breach-managing-employees-during-a-data-incident.

D Kahneman. A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, 58(9):697–720, 2003. https://doi.org/10.1037/0003-066X.58.9.697.

Daniel. Katz and Robert L. Kahn. *The Social Psychology of Organizations*. New York, USA: John Wiley & Sons, 2 edition, 1978.

Tina Kiefer. Feeling bad: Antecedents and consequences of negative emotions in ongoing change. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, 26(8):875–897, 2005. https://doi.org/10.1002/job.339.

Tina Kiefer and Laurie J Barclay. Understanding the mediating role of toxic emotional experiences in the relationship between negative emotions and adverse outcomes. *Journal of Occupational and Organizational Psychology*, 85(4):600–625, 2012. https://doi.org/10.1111/j.2044-8325.2012.02055.x.

Peter H Kim, Donald L Ferrin, Cecily D Cooper, and Kurt T Dirks. Removing the shadow of suspicion: the effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of Applied Psychology*, 89(1):104–114, 2004. https://doi.org/10.1016/j.obhdp.2005.07.002.

P.H. Kim, K.T. Dirks, C.D. Cooper, and D.L. Ferrin. When more blame is better than less: The implications of internal vs. external attributions for the repair of trust after a competence-vs. integrity-based trust violation. *Organizational Behavior and Human Decision Processes*, 99(1):49–65, 2006. https://doi.org/10.1016/j.obhdp.2005.07.002.

P.H. Kim, C.D. Cooper, K.T. Dirks, and D.L. Ferrin. Repairing trust with individuals vs. groups. *Organizational Behavior and Human Decision Processes*, 120(1):1–14, 2023. https://doi.org/10.1016/j.obhdp.2012.08.004.

Ulla Kinnunen, Taru Feldt, Marjaana Sianoja, Jessica de Bloom, Kalevi Korpela, and Sabine Geurts. Identifying long-term patterns of work-related rumination: Associations with job demands and well-being outcomes. *European Journal of Work and Organizational Psychology*, 26(4):514–526, 2017. https://doi.org/10.1080/1359432X.2017.1314265.

Audrey Korsgaard and Paul Bliese. Divergence in collective trust. In Nicole Gillespie, C. Ashley Fulmer, and Roy J. Lewicki, editors, *Understanding Trust in Organizations: A Multilevel Perspective*, chapter 3, pages 45–65. Routledge, 2021.

Audrey M. Korsgaard, J. Kautz, P. Bliese, K. Samson, and P. Kostyszyn. Conceptualising time as a level of analysis: New directions in the analysis of trust dynamics. *Journal of Trust Research*, 8(2):142–162, 2018. https://doi.org/10.1080/21515581.2018.1516557.

M Audrey Korsgaard, Susan E Brodt, and Ellen M Whitener. Trust in the face of conflict: The role of managerial trustworthy behavior and organizational context. *Journal of Applied Psychology*, 87(2):312–319, 2002. https://doi.org/10.1037/0021-9010.87.2.312.

Ravie Lakshmanan. Solarwinds blames intern for 'solarwinds123' password lapse, 2021. https://thehackernews.com/2021/03/solarwinds-blame-intern-for-weak.html.

Yael Lapidot, Ronit Kark, and Boas Shamir. The impact of situational vulnerability on the development and erosion of followers' trust in their leader. *The Leadership Quarterly*, 18(1):16–34, 2007. https://doi.org/10.1016/j.leaqua.2006.11.004.

Elmer E.H. Lastdrager. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3:1–10, 2014. https://doi.org/10.1186/s40163-014-0009-y.

Dora C Lau, Long W Lam, and Shan S Wen. Examining the effects of feeling trusted by supervisors in the workplace: A self-evaluative perspective. *Journal of Organizational Behavior*, 35(1):112–127, 2014. https://doi.org/10.1002/job.1861.

Richard S Lazarus and Susan Folkman. *Stress, appraisal, and coping*. Springer Publishing Company, 1984.

Jonathan I Lee, Kurt T Dirks, and Rachel L Campagna. At the heart of trust: Understanding the integral relationship between emotion and trust. *Group & Organization Management*, 48(2):546–580, 2023. https://doi.org/10.1177/10596011221118499.

Timothy B. Lee. The sony hack: how it happened, who is responsible, and what we've learned, 2014. https://www.vox.com/2014/12/14/7387945/sony-hack-explained.

A. Legood, L. van der Werff, A. Lee, D. den Hartog, and D. van Knippenberg. A critical review of the conceptualization, operationalization, and empirical literature on cognition-based and affect-based trust. *Journal of Management Studies*, 60(2):495–537, 2023. https://doi.org/10.1111/joms.12811.

Elizabeth A Lemerise and William F Arsenio. An integrated model of emotion processes and cognition in social information processing. *Child Development*, 71(1):107–118, 2000. https://doi.org/10.1111/1467-8624.00124.

Jennifer S Lerner, Ye Li, Piercarlo Valdesolo, and Karim S Kassam. Emotion and decision making. *Annual Review of Psychology*, 66:799–823, 2015. https://doi.org/10.1146/annurev-psych-010213-115043.

J David Lewis and Andrew Weigert. Trust as a social reality. *Social Forces*, 63(4):967–985, 1985. https://doi.org/10.1093/sf/63.4.967.

Sally Maitlis and Marlys Christianson. Sensemaking in organizations: Taking stock and moving forward. *Academy of Management Annals*, 8(1):57–125, 2014. https://doi.org/10.5465/19416520.2014.873177.

Alex Mathers. Protecting business value with cyber security, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of Management Review*, 20(3):709–734, 1995. https://doi.org/10.5465/amr.1995.9508080335.

D.J. McAllister. Affect and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, 38(1):24–59, 1995. https://doi.org/10.5465/256727.

Shiona McCallum. Uber investigating hack on its computer systems, 2022. Retrieved 9 July 2023 from: https://www.bbc.co.uk/news/technology-62925047.

D Harrison McKnight, Larry L Cummings, and Norman L Chervany. Initial trust formation in new organizational relationships. *Academy of Management Review*, 23(3):473–490, 1998. https://doi.org/10.5465/amr.1998.926622.

Susan Michie and Janaki Gooty. Values, emotions, and authenticity: Will the real leader please stand up? *The Leadership Quarterly*, 16(3):441–457, 2005. https://doi.org/10.1016/j.leaqua.2005.03.006.

Dan Milmo. NHS ransomware attack: what happened and how bad is it?, 2022. Retrieved 9 July 2023 from: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it.

Barbara A Misztal. Trust: Acceptance of, precaution against and cause of vulnerability. In Masamichi Sasaki and Robert M. Marsh, editors, *Trust*, pages 209–236. Brill, 2012. https://doi.org/10.1163/9789004221383_010.

Lawrence B Mohr. *Explaining Organizational Behavior: The Limits and Possibilities of Theory and Research.* Jossey-Bass, San Francisco, USA, 1982.

Frederick P Morgeson, Terence R Mitchell, and Dong Liu. Event system theory: An event-oriented approach to the organizational sciences. *Academy of Management Review*, 40(4):515–537, 2015. https://doi.org/10.5465/amr.2012.0099.

Ellen Nakashima and Philip Rucker. U.S. declares North Korea carried out massive WannaCry cyber-attack, 2017. https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html (Accessed 2018).

C.G Nerstad, R Searle, M Černe, A Dysvik, M. Škerlavaj, and R Scherer. Perceived mastery climate, felt trust, and knowledge sharing. *Journal of Organizational Behavior*, 39(4):429–447, 2018. https://doi.org/10.1002/job.2241.

Ka Chung Ng, Xiaojun Zhang, James YL Thong, and Kar Yan Tam. Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, 38(3):732–764, 2021. https://doi.org/10.1080/07421222.2021.1962601.

Ann-Marie Nienaber, Marcel Hofeditz, and Philipp Daniel Romeike. Vulnerability and trust in leader-follower relationships. *Personnel Review*, 44(4):567–591, 2015. https://doi.org/10.1108/PR-09-2013-0162.

Jason RC Nurse, Oliver Buckley, Philip A Legg, Michael Goldsmith, Sadie Creese, Gordon RT Wright, and Monica Whitty. Understanding insider threat: A framework for characterising attacks. In *IEEE Security and Privacy Workshops*, pages 214–228. IEEE, 2014. https://doi.org/10.1109/SPW.2014.38.

Michael D Pfarrer, Katherine A Decelles, Ken G Smith, and M Susan Taylor. After the fall: Reintegrating the corrupt organization. *Academy of Management Review*, 33(3):730–749, 2008.

Daniel Pienta, Jason Bennett Thatcher, and Allen Johnston. Protecting a whale in a sea of phish. *Journal of Information Technology*, 35(3):214–231, 2020. https://doi.org/10.1177/0268396220918594.

Karen Renaud and Marc Dupuis. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*, pages 42–56, Costa Rica, 2019. https://doi.org/10.1145/3368860.3368864.

Karen Renaud, Alfred Musarurwa, and Verena Zimmermann. Contemplating blame in cyber security. In *16th International Conference on Cyber Warfare and Security (ICCWS)*, pages 309–317. Academic Conferences Limited, 2021a.

Karen Renaud, Verena Zimmermann, Tim Schürmann, and Carlos Böhm. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 8(1):1–17, 2021b.

Karen Renaud, Rosalind Searle, and Marc Dupuis. Cybersecurity regrets: I've had a few.... je ne regrette. In *Proceedings of the 2022 New Security Paradigms Workshop*, pages 1–20, 2022. https://doi.org/10.1145/3584318.3584319.

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

L Ritzenhöfer, P Brosi, M Spörrle, and IM Welpe. Leader pride and gratitude differentially impact follower trust. *Journal of Managerial Psychology*, 32(6):45–459, 2017. https://doi.org/10.1108/JMP-08-2016-0235.

Pierangelo Rosati, Peter Deeney, Mark Cummins, Lisa Van der Werff, and Theo Lynn. Social media and stock price reaction to data breach announcements: Evidence from us listed companies. *Research in International Business and Finance*, 47:458–469, 2019. https://doi.org/10.1016/j.ribaf.2018.09.007.

L Ross. Trust: The intuitive psychologist and his shortcomings: Distortions in the attribution process. In L Berkowitz, editor, *Advances in Experimental Social Psychology*, volume 10, pages 173–220. Academic Press:New York, 1977.

Gerald R Salancik and Jeffrey Pfeffer. A social information processing approach to job attitudes and task design. *Administrative Science Quarterly*, 23(2):224–253, 1978. https://doi.org/10.2307/2392563.

Rosalind H. Searle. Trust and HRM. In Sim B. Sitkin Rosalind H. Searle, Ann-Marie I. Nienaber, editor, *The Routledge Companion to Trust*, pages 483–505. Routledge, 2018.

Rosalind H Searle and Charis Rice. Making an impact in healthcare contexts: insights from a mixed-methods study of professional misconduct. *European Journal of Work and Organizational Psychology*, 30(4):470–481, 2021. https://doi.org/10.1080/1359432X.2020.1850520.

Rosalind H Searle and Charis Rice. Trust, and high control: an exploratory study of counterproductive work behaviour in a high security organization. *European Journal of Work and Organizational Psychology*, pages 1–11, 2024. In Press.

Gabi Siboni and David Siman-Tov. Cyberspace Extortion: North Korea versus the United States, 2014. December 23 INSS Insight No. 646, http://www.inss.org.il/publication/cyberspace-extortion-north-korea-versus-the-united-states/ (Accessed 7/1/2019).

T Simons, H Leroy, V Collewaert, and S Masschelein. Low leader alignment of words and deeds affects followers: A meta-analysis of behavioral integrity research. *Journal of Business Ethics*, 132:831–844, 2015. https://doi.org/10.1007/s10551-014-2332-3.

Mikko Siponen. Stage theorizing in behavioral information systems security research. In *Hawaii International Conference on System Sciences*, Honolulu, 3-6 January, 2024. https://hdl.handle.net/10125/106952.

D.P. Skarlicki, L.J. Barclay, and D.S. Pugh. When explanations for layoffs are not enough: Employer's integrity as a moderator of the relationship between informational justice and retaliation. *Journal of Occupational and Organizational Psychology*, 81(1):123–146, 2008. https://doi.org/10.1348/096317907X206848.

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

Gretchen M Spreitzer and Aneil K Mishra. To stay or to go: Voluntary survivor turnover following an organizational downsizing. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, 23(6):707–729, 2002. https://doi.org/10.1002/job.166.

Patrick Stacey, Rebecca Taylor, Omotolani Olowosule, and Konstantina Spanaki. Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management*, 58:102298, 2021. https://doi.org/10.1016/j.ijinfomgt.2020.102298.

Alexander Staves, Tom Anderson, Harry Balderstone, Benjamin Green, Antonios Gouglidis, and David Hutchison. A cyber incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection*, 37:100505, 2022. https://doi.org/10.1016/j.ijcip.2021.100505.

Josh Taylor. Medibank hack started with theft of company credentials, investigation suggests, 2022. Retrieved 9 July 2023 from: https://www.theguardian.com/technology/2022/oct/24/medibank-hack-started-with-theft-of-staff-members-credentials-investigation-suggests.

Edward C Tomlinson and Roger C Mryer. The role of causal attribution dimensions in trust repair. *Academy of Management Review*, 34(1):85–104, 2009. https://doi.org/10.5465/amr.2009.35713291.

William Turton and Kartikay Mehrotra. Hackers Breached Colonial Pipeline Using Compromised Password, 2021. https://www.inflexion.com/news-insights-events/inflexion-exchange/2021/protecting-business-value-with-cyber-security/.

Chris Vallance. Twitter: Millions of users' email addresses 'stolen' in data hack, 2023. Retrieved 9 July 2023 from: https://www.bbc.co.uk/news/technology-64153381.

Steve G.A. van de Weijer, Rutger Leukfeldt, and Sophie van der Zee. Cybercrime reporting behaviors among small-and medium-sized enterprises in the netherlands. In *Cybercrime in Context: The human factor in victimization, offending, and policing*, pages 303–325. Springer, 2021.

Bessel Van der Kolk. *The body keeps the score: Mind, brain and body in the transformation of trauma.* Penguin, UK, 2014.

Lisa van der Werff, Alison Legood, Finian Buckley, Antoinette Weibel, and David de Cremer. Trust motivation: The self-regulatory processes underlying trust decisions. *Organizational Psychology Review*, 9(2-3):99–123, 2019. https://doi.org/10.1177/2041386619873616.

Lisa van der Werff, Deirdre O'Shea, Graham Healy, Finian Buckley, Colette Real, Michael Keane, and Theo Lynn. The neuroscience of trust violation: Differential activation of the default mode network in ability, benevolence and integrity breaches. *Applied Psychology*, 72(4):1392–1408, 2023. https://doi.org/10.1111/apps.12437.

Gerben A Van Kleef. How emotions regulate social life: The emotions as social information (EASI) model. *Current Directions in Psychological Science*, 18(3):184–188, 2009. https://doi.org/10.1111/j.1467-8721.2009.01633.x.

Gerben A Van Kleef. Understanding the positive and negative effects of emotional expressions in organizations: EASI does it. *Human Relations*, 67(9):1145–1164, 2014. https://doi.org/10.1177/0018726713510329.

Stéphane van Kleef, Gerben A. & Côté. The social effects of emotions. *Annual Review of Psychology*, 73: 629–658, 2022. https://doi.org/10.1146/annurev-psych-020821-010855.

Daan Van Knippenberg. Reconsidering affect-based trust: A new research agenda. In *The Routledge Companion to Trust*, chapter 1, pages 3–13. Routledge, 2018.

Bart S Vanneste, Phanish Puranam, and Tobias Kretschmer. Trust over time in exchange relationships: Meta-analysis and theory. *Strategic Management Journal*, 35(12):1891–1902, 2014. https://doi.org/10.1002/smj.2198.

Shubhendu Vatsa. 'Fake CFO': $25 Million Deepfake Video Call Scam Rocks Hong Kong Company, 2024. https://www.msn.com/en-au/money/news/fake-cfo-25-million-deepfake-video-call-scam-rocks-hong-kong-company/ar-BB1i3O5G.

Yvonne Villarreal. Sony employees receive threatening email, allegedly from hackers, 2014. https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-employees-email-from-hackers-20141205-story.html.

Ido Vock. 'No need to apologise' for leaked call - German ambassador to UK, 2024. https://www.bbc.co.uk/news/world-europe-68488962.

D Watson, D Wiese, J Vaidya, and A Tellegen. The two general activation systems of affect: Structural findings, evolutionary considerations, and psychobiological evidence. *Journal of Personality and Social Psychology*, 75 (5):820–838, 1999. https://doi.org/10.1037/0022-3514.76.5.820.

Antoinette Weibel, Deanne N Den Hartog, Nicole Gillespie, Rosalind Searle, Frédérique Six, and Denise Skinner. How do controls impact employee trust in the employer? *Human Resource Management*, 55(3):437–462, 2016. https://doi.org/10.1002/hrm.21733.

Antoinette Weibel, Simon Schafheitle, and Lisa van der Werff. Smart tech is all around us – bridging employee vulnerability with organizational active trust-building. *Journal of Management Studies*, 2023. https://doi.org/10.1111/joms.12940 In Press.

Elizabeth Weise. A timeline of events surrounding the Equifax data breach, 2024. https://eu.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/.

Mathew P White, Sabine Pahl, Marc Buehner, and Andres Haye. Trust in risky messages: The role of prior attitudes. *Risk Analysis: An International Journal*, 23(4):717–726, 2003. https://doi.org/10.1111/1539-6924.00350.

E.M Whitener, S.E. Brodt, M.A Korsgaard, and J Werner. Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior. *Academy of Management Review*, 23(3):513–530, 1998. https://doi.org/10.5465/amr.1998.926624.

Ben Wilson. Lastpass security breach leaked encrypted customer password vaults, 2022. https://www.windowscentral.com/software-apps/lastpass-security-breach-encrypted-customer-vaults.

Josephine Wolff. *You'll see this message when it is too late: The Legal and Economic Aftermath of Cybersecurity Breaches*. MIT Press, Cambridge, MA, 2018.

Chul Woo Yoo, Jahyun Goo, and H Raghav Rao. Is cybersecurity a team sport? a multilevel examination of workgroup information security effectiveness. *MIS Quarterly*, 44(2), 2020. 10.25300/MISQ/2020/15477.

Verena Zimmermann and Karen Renaud. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131:169–187, 2019. https://doi.org/10.1016/j.ijhcs.2019.05.005.