STACEY CONCHIE

TRUST IN SECURITY CONTEXTS

Guest editor Professor Stacey Conchie provides an overview of the articles focusing on our special topic of trust.

"To trust, or not to trust, that is the question."

When we interact with a person, group, organisation or system, we may ask this question. We may not consciously verbalise this question and nor will we stick with a relationship because of a fear of what comes if we leave through distrust. Yet, the opening line of Hamlet's soliloquy captures the process that people go through when deciding whether to join, remain or exit a relationship.

What does it mean to trust? When a person trusts another (the trustee), they will accept vulnerability by relying on the trustee to do something of value, which affects them, yet which they have no control over. If we can predict the trustee's actions, then the situation does not call for trust. A person often has more to lose from trusting and being betrayed than from the gains of trust being fulfilled. A covert source may gain financially if their handler is trustworthy. However, if their handler is untrustworthy and betrays them, the consequence may be imprisonment or a threat to their life. For this reason, trust is a risky business.

> **A person often has more to lose from trusting and being betrayed than from the gains of trust being fulfilled.**

Trust (i.e., a willingness to accept vulnerability) is strongly related to a person's beliefs about another's trustworthiness. Indeed, trust and trustworthiness are often synonymous in the literature. Many individual qualities have been proposed to indicate how trustworthy a trustee is. The well-used framework of Mayer and colleagues groups these qualities into those that reflect a trustee's ability, their integrity, and their benevolence. Some researchers go one step further and propose a dichotomy, where ability sits on one side and integrity and benevolence on the other. Beliefs about the former are more rational and objective, the latter more emotional and subjective. As we see in this issue of CSR, both are implicated in security contexts. However, the scale shows a bias towards the subjective end (weighted by integrity) when it comes to shaping behaviour.

Several factors influence trust, including personality, cognitive biases (e.g., stereotypes), similar—past—relationships, gossip, appearance, and direct experience with the trustee. Not all factors are equal in their influence. Nor do they have a prevailing effect. For example, personality (or a person's readiness to trust) is most influential when we meet a potential trustee for the first time, but weakens as we interact with them and observe how they treat others. Trust is not static. The base on which it develops changes and with this, so does its relative influence on risk taking.

This issue of CSR looks at trust in different contexts. The first set of papers look at the role of trust in elicitation. Lina Hillner theorises on the difference between rapport and trust. Anna Leslie and Simon Wells draw on the Eliciting Information Framework to illustrate how this distinction plays out at a practical level. Andreea-Antonia Raducu compares trust against similarity and empathy in the context of a source handler-informant life-cycle.

Stacey Conchie and Paul Taylor show us that not all trust judgements occur at a conscious level. They document studies that show how we might capture people's automatic trust judgements through nonverbal and verbal behaviours.

> **If we can predict the trustee's actions, then the situation does not call for trust.**

We then consider what happens when trust is threatened. Emma Barrett summarises betrayal research and shows how security contexts are hotbeds for their occurrence. One outcome of betrayal is distrust, which in some contexts (e.g., disengagement and deradicalisation) can have positive outcomes (see Morrison et al.), but in others can cause retaliation behaviours that pose security risks, as seen with insider attacks. Rosalind Searle draws on her CREST research to illustrate how trust can be damaged within organisations through poor leadership and how this may be avoided. Steven Lockey discusses how trust may be repaired following a breach (e.g., betrayal), and, similar to the work conducted by Mariam Oostinga on communication errors, shows the important role of an apology. He extends this to illustrate the need for concomitant structural changes when a violation occurs at an organisational level.

Trust not only occurs between people. Ella Glikson illustrates this by summarising research on the role of emotional and rational trust in AI. Paul Taylor discusses the importance of trusting research centres. Finally, Calvin Burns points to the role of trust between organisations (and the many forms trust can take) in a concluding A-Z of trust.

The collection of trust articles in the current (and previous issues of) CSR provide a glimpse into the multi-faceted nature of trust. The coverage is not exhaustive, but all agree on its importance. There is certainly much more to be known about trust in this area and we will continue to see new and innovative work around trust in security contexts as we move forward.

Stacey Conchie is a professor in psychology at Lancaster University and Director of CREST.

Image credit: *ASDF* | stock.adobe.com