



Choice Architecture and Organisational SRM Buy-in

Araba Cole and Panagiotis Olympiou

Introduction

Choice architecture is the deliberate design of the context in which choices are offered to a targeted group of people, and it is the responsibility of the choice architect – in this case, the SRM practitioner – to facilitate or hinder desired behaviours through the way in which choices are presented (Thaler & Sunstein, 2008). Choice architecture is used in multiple areas, such as government and advertising¹, to facilitate the desired behaviour of targeted groups. This article explores how choice architecture can be adapted to increase SRM buy-in within humanitarian organisations, which we consider essential to strengthen the acceptance component of the organisation's SRM strategy.

SRM buy-in from within an organisation and its staff at all levels is essential both to preserving the wellbeing of personnel and to support their ability to deliver effective, do no harm programming. In turn, achieving these objectives helps to safeguard an organisation's acceptance by external actors. If buy-in is not achieved, individual actions as well as organisational shortcomings in the implementation of an otherwise sound SRM approach can affect both an organisation's results and perceptions of their operation and delivery. Therefore, maximizing buy-in from within can play a significant role in both the robustness of SRM per se as well as acceptance more broadly. Choice architecture – along with other aspects of cognitive and behavioural research – can help explain why buy-in sometimes fails, and provide insights and practices to help increase it.

Fundamental to both SRM buy-in and acceptance by external actors is perception: perceptions guide behaviour, and behaviour shapes individual choices (Kahneman 2013). The technical aspects of SRM – which come in the form of standard operating

procedures (SOPs), guidelines, etc. – often do not account for *actual* human behaviour or fluctuations in personal diligence. While SRM may correctly identify security risks and propose logically coherent solutions, these solutions are not always followed by individuals, which often turns out to be the weakest link of the SRM chain. There are two ways in which SRM can engage with the human element to improve organisational buy-in: addressing perceptions, and utilising choice architecture. SRM professionals can address staff perceptions of SRM by considering the following questions. Do staff also see risk where the security professionals do? Do staff consider the measures implemented to be commensurate to programmatic objectives? Do external stakeholders perceive the organisations' activities as aligned with the do no harm principle? Perceptions are often a target of security professionals, who try to influence these by means of communication, training, and as a last resort, human resources measures (verbal or written warnings, termination of contracts or other disciplinary actions as a result of not adhering to the security protocols of an organisation's actions). While work on perceptions is important, it is also fleeting in a domain that is very dynamic, results-driven, and characterized by high staff turnover within missions. These approaches are thus not failsafe, and they may leave behaviours unaltered with little other recourse available to ensure buy-in throughout the organisation, hence the importance of choice architecture as another means of improving buy-in.

Instead of targeting staff perceptions, knowledge or skills, choice architecture aims at intervening in the environment in which staff operate, and so directly affects their behaviour. Instead of solely seeking to change behaviours by instruction, it *induces* the desired behaviours by offering a particular choice or set of choices, in a particular way. We propose that

¹ Choice architecture has already been deployed very successfully in other sectors. Thaler & Sunstein (2008) developed the concept of the 'nudge' which has gone on to see practical application in the UK government by David Halpern who led the 'Nudge Unit' or, more formally, the Behavioural Insights Team. By capitalizing on behavioural insights and cognitive biases they had significant successes in affecting citizens' decision-making to help improve results in areas such as tax collection and unemployment. Another arena where such understanding has paid enormous dividends is in marketing and advertising (Shotton 2018), and data on consumer choices is becoming one of the biggest commodities on the market (Matsakis 2019, Melendez & Pasternack 2019).

this approach is both essential and complementary to other SRM techniques, as it facilitates better organisational buy-in which in turn enables the safe and effective program delivery essential for sustained acceptance by external actors throughout the program lifecycle.

Our analysis begins by examining the limitations and obstacles to SRM buy-in within organisations, taking into account issues of perception, communication, and resourcing surrounding security risk management. We then look at relevant research and its value to NGO SRM. Finally, we demonstrate how the learning from these research reports can be applied to SRM practices in NGOs in order to gain stronger organisational buy-in.

Obstacles to organisational buy-in

In and of itself, SRM can be a burden to the operations of NGOs. Many staff see the implementation of SRM as detracting resources from their primary objective: program implementation. Notably, SRM often requires staff members to adjust their behaviour in a way that may be additional and external to their self-perceived core professional identity (be it a logistician, a protection expert, a humanitarian, a programme manager, or other). Moreover, SRM might call for a set of everyday (and often mundane) actions, which are implemented differently in the professional setting than in the private life of the same individual (e.g. locally hired staff driving organisational vehicles wearing seat belts, but not while driving their personal vehicles). Moreover, under time and other constraints, even diligent employees can find themselves downgrading security tasks when demands more central to their job function become urgent.

Not only can SRM be expensive and obtuse, but it can also be hard to persuade people of the value of good SRM. NGOs often lack the key metrics used to evaluate SRM performance as seen in other sectors, such as returns on investment (RoI) and return on prevention (RoP).² There is effectively a problem of negative proof: how to prove something (e.g., a major security incident) did *not* happen as a result of SRM efforts. Fundamentally, as a result of slim incentives, the significant effort and resources required, and

a conscious or unconscious lack of prioritisation, staff and managers do not always make choices conducive to successful SRM and acceptance. Choice architecture, with its foundational principles of behavioural insights and cognitive biases, can be used to remedy this.

Leveraging biases

At the heart of choice architecture is the fundamental concept that humans are not always rational decision-makers: we do not necessarily automatically choose of our own volition what is safest for us or what serves our larger and long-term objectives. We are, in fact, human, and our choices and behaviour deviate from logical expectations, and these deviations provide the space for choice architecture. In our case, where compliance and buy-in of SRM may seem logical in insecure operating environments, this is not always the norm. Significant work has been done in identifying how human behaviour deviates from a rational norm, particularly in the face of risk, in the form of cognitive biases (Taleb 2018). We will outline here some of these biases and what they can look like, and in the next section indicate how choice architecture can be used to help overcome them and improve SRM buy-in.

One of these biases, *loss aversion*, has been highlighted as a key motivator in decision making. In the face of certain loss, most people prefer a gamble, while in the face of certain gain, a gamble is very unattractive. For example, the security arm of an organisation wishes to install a new warehouse locking system to prevent possible theft, but the budget holder is willing to gamble that such theft will not occur and declines to authorise the expense (which is seen as a certain loss). Loss aversion can be a significant obstacle to SRM buy-in, with security measures being seen as a loss of time, money, energy, and sometimes all three. However, once we understand what loss aversion is and how it influences behaviour, we can use choice architecture to present the choice differently (even if the choice is a simple Yes or No – in the example above, funding or not funding the locking system). Framing a choice of behaviour on the basis of “gains or losses relevant to the status quo” (Kahneman and Tversky, 1984:343) can impact on the choice made. In the

² As a performance indicator, return on investment (RoI) evaluates the economic benefit of an investment, as compared to the investment's cost. Return of prevention (RoP) measures an organisation's economic benefit deriving from ensuring occupational safety and health. Examples of such investment pertaining to SRM could be hostile environment awareness training (HEAT) or hands-on personal safety courses, physical security installations like automatic locks, or medical evacuation and kidnap and ransom insurance.

example above, framing the installation of the new warehouse locking system as an investment which will save an organisation thousands of dollars in misappropriated stock rather than solely presenting the initial cost of the new system will be much more attractive to the budget holder and decision makers involved.

Similarly, the *fundamental attribution error* describes people's tendency to explain an individual's behaviour by attributing her actions to her personality, while simultaneously underestimating the significance of contextual and situational factors at play (Shotton 2018). Although instinct leads us to almost always believe that a behaviour is the result of one's character, social psychology experiments (Jones & Harris 1967) have shown this to be a fallacy, and that context or specific situation affects behaviour to a greater extent than we intuitively perceive. For instance, an NGO driver in rural Lebanon who fails to carry out desired SOPs at a checkpoint despite his training and instruction by management may at first instance appear to be negligent. However, upon closer inspection he may well be responding to a feature of the environment: his social ties with checkpoint personnel may oblige him to adhere to social expectations rather than organisational SOPs. Incorporating this insight into one's analysis and systems design allows for a more nuanced understanding of behavioural causes, thus opening up a wide range of opportunities for achieving the desired results by moving the focus from the individual to the environment in which she operates. While there is not one answer on whether adhering to all local social norms necessarily safeguards an organisation's acceptance, misalignments between SRM protocols and employees' behaviour flag points of friction to the SRM practitioner designing procedures.

Our perception of risks can also be similarly fickle. When thinking about risks such as causes of fatalities or assessing how dangerous something is, we often conjure images and information that we might have recently been exposed to, for instance in omnipresent social media or news. This is an example of the *availability heuristic*³ (Kahneman & Tversky 1974) which prompts us to reach for the most readily available and vibrant information to answer a question or solve a problem. For example,

let's consider a delegation of donors who had planned to visit a provincial capital in Eastern Afghanistan by road. During the fortnight before their travel, improvised explosive device attacks on this road increased from one to three, a development which led the delegation to seriously consider cancelling their visit, despite the fact that similar or even higher numbers of such attacks had been seen in multiple instances during the previous year. The fact that this relative spike was recent, however, had a disproportionate impact on the delegation's perception of insecurity, despite all other factors pointing to a normal level of risk. Once again, knowledge of this cognitive bias can provide an opportunity to SRM practitioners to ensure that relevant SRM information is salient in the minds of those choosing a course of action, and help balance the effect of recent and vibrant information in decision making.

The *representativeness heuristic* (Kahneman & Tversky 1974) is another bias that can cause blindness to risk. If something is representative of or looks like something that is safe or normal, then we are unlikely to respond; if it doesn't look like our archetypes of a threat or a danger, then we are unlikely to challenge or mitigate against it. From an SRM perspective, this can cause a critical myopia when dealing with risk, which can manifest itself as resistance to SRM by personnel within an organisation; potential threats and hazards may not always be easily recognisable and so a plan to mitigate them may be challenging to justify or enforce. This has been a significant challenge in Afghanistan, where female suicide bombers were highly effective due to women not being seen as threatening, as well as cultural barriers against searching women (either by men, or the hiring of female guard personnel). Women were not *representative* of the threat, nor were they representative of the solution.

Though it may be rational to support organisational SRM in order to facilitate safe and responsible programming and acceptance by stakeholders, this is not always the reality due to some of the deeply ingrained cognitive hardwiring described above. Choice architecture enables SRM practitioners to overcome some of these biases to help increase effectiveness and buy-in of their SRM measures. We will examine some key uses in the next section.

³ A heuristic is a means of problem solving that utilises an approximation or 'rule of thumb' rather than an optimal solution.

Uses for the SRM practitioner

In a world where trying to generate SRM buy-in can often feel like trying to sell an unpopular product to a hostile market, these insights are of significant value to the SRM practitioner who wishes to increase buy-in, make programmes safer, and gain the trust and acceptance of stakeholders. Here are a few examples:

- Choice architecture methods can be used to increase the likelihood that SRM measures – e.g. SOPs, physical security measures – are adopted by making them easy, attractive, social, and timely (the ‘EAST’ principle, Halpern 2015). If the desired behaviour – for instance, incident reporting by staff in the field – is unattractive, challenging, or inconvenient then it is unlikely to be carried out. As security practitioners we must think about making the desired choice the one that meets the least resistance. Rather than security incident reporting being laborious, bureaucratic, or incurring punishment if staff fail to complete it, incident reporting could be made available via the most convenient means for the staff member (e.g. WhatsApp voice note), and in a format that is simple and convenient. Doing so would be a point of *reward* by management, and with the EAST principle in mind, reporting on incidents would be far more likely to be carried out. This can be reinforced with positive messaging to staff that praises swift incident reporting, and explains how they have contributed to organisational safety.

Organisations can use this principle not only internally, but also to maximise the external feedback which is essential for a successful acceptance SRM approach. All too often, feedback mechanisms such as affected communities’ feedback and grievance redress mechanisms are under-used due to a lack of behavioural insight; choice architecture (like EAST) can vastly improve such mechanisms, providing organisations with the grassroots understanding vital to maintaining an effective acceptance approach.

- Rather than resistance to proposed SRM approaches being an amorphous feature of security within NGOs, we now have the insights to better understand the points of friction that can result from cognitive biases and their corresponding perceptions and behaviours. Through better understanding of resistance points or the shortcomings of measures, it is easier to overcome them and thus increase buy-in. For

instance, when there is a singular high-profile incident within a context (an outlier event, such as a kidnapping of a foreign national in Kabul), it is common to see disproportionate organisational reactions that are at odds with SRM advice (such as the widespread implementation of curfews despite no evidence of incidents being more likely at night). This is an example of the *availability heuristic* at work, where a vibrant and recent dramatic event becomes the driver of decision-making rather than a holistic consideration of the wider context. Individual reactions can then be reinforced and perpetuated by *social-proofing* as such measures gain traction across the wider NGO community. Being aware that such biases and errors are at play, an SRM practitioner now knows that she must address these heuristics in her communication with management, providing broad and balanced information, to help counter the visceral impact of a high-profile recent event on choices made. This can be achieved through regular security and context briefings, either dedicated or bolted on to existing management meetings, as well as other forms of regular security communications such as weekly reporting and circulation of relevant articles and analysis.

- Context, not only personal attributes such as role or disposition, can be utilised as a part of a choice architecture approach in SRM. By considering the context in which safety and security decisions and behaviours take place, practitioners can better understand staff members’ choices. While the exact adaptations of SRM policy will differ from one case to another, the cognitive process remains constant. For example, group-thinking in a large stakeholder engagement meeting may undermine the nuances of an NGO’s proposal, where multiple members of the local community have competing interests. By choosing a more amenable context, such as bilateral discussions with individual stakeholders in more relaxed settings, the interlocutor is better placed to create a more conducive context and gain greater acceptance, thus contributing to the safety of the NGO’s operations.
- Choice architecture can be used to combat cognitive biases that cause myopia towards risk when dealing with outlier, high impact, extremely low probability events, known as *black swans* (Taleb 2007). When framing our choices and decisions we are prone to fixate narrowly on a single course of events without

a wider perception of other outcomes, and are thus vulnerable to a host of biases. *Confirmation bias*⁴ as well as the *What You See Is All There Is*⁵ bias, can be debilitating to contingency planning and crisis management, as they fail to allow for maximum perception of and adaptation to future developments. Using exercises such as Heuer's *Analysis of Competing Hypotheses* can actively account for such biases and can widen the perspective of management when making choices under uncertainty (Heuer 1999). This can lead to more robust decision-making that incorporates a greater spectrum of outcomes, for instance when crisis management teams consider critical incidents or significant contextual developments like elections or even aggressive transitions of power. Failure in the face of critical, rare incidents is a common, albeit unrepresentative, critique to acceptance of SRM approaches, and success in this arena can greatly enhance not only organisational buy-in in the future, but also stakeholders' and communities' trust in organisational resilience, further increasing acceptance.

- Finally, a key lesson from the methodologies used in the application of choice architecture is to consider, measure, and observe peoples' *actual* behaviour, rather than what one thinks is obvious, or imagines what people *should* be doing. Therefore, SRM practitioners could greatly benefit from gaining additional understanding of the reasons driving undesired behaviour: *why* are safety procedures not being followed by staff? *Why* do management fail to integrate safety and security concerns in proposal and project design? To gain insight into these questions, SRM practitioners can use structured observation, small scale experiments, and testing of their hypotheses in different configurations of individual and group settings. Experimentation and testing not only clarifies the reasons behind the shortcomings of SRM measures, but it also engages staff and management, thus generating ownership. Introspection and the involvement of staff increases buy-in through the very process of gaining understanding.

Conclusion

Thinking and research on cognitive biases such as loss aversion, the availability and representativeness heuristics, and fundamental attribution errors can shed light on obstacles to SRM buy-in within an organisation. Armed with this knowledge, we can adjust security practices to target these obstacles, using aspects of choice architecture to facilitate desired behaviours, choices, and decisions from staff and other actors, which also helps increase acceptance. After all, acceptance as an SRM strategy often faces challenges stemming from failures to implement technical aspects of SRM. Choice architecture can equip SRM practitioners with actionable means to increase technical successes, thus maximising the organisational buy-in of security programming, including acceptance strategies.

This article presents only a fraction of the concepts and research conducted on behavioural insights, and its application in choice architecture. It does nonetheless demonstrate the role of SRM practitioners as choice architects who can utilise behavioural insights to enrich their practice and invigorate organisational buy-in of SRM strategies. This in turn leads to the safer and more effective delivery of aid and greater acceptance by stakeholders.

⁴ The confirmation bias refers to the habit of using new information to confirm rather than challenge or disprove existing beliefs, opinions or hypotheses (Oswald, M. & Grosjean, S 2004).

⁵ *What You See Is All There Is* refers to the propensity to make decisions without considering the existence of known unknowns or unknown unknowns (Kahneman 2011).

Bibliography

Cialdini, R. (1984). *Influence: Science and Practice*. New York, HarperCollins College Publishers.

Halpern, D. (2015). *Inside the Nudge Unit: How Small Changes Can Make a Big Difference*. London, Random House.

Heuer, R. (2001) [1999]. *Psychology of Intelligence Analysis* (2nd ed.). Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.

Jones, E. E., & Harris, V. A. (1967). The attribution of attitudes. *Journal of experimental social psychology*, 3(1), 1-24.

Kahneman, D. & Tversky, A. (1974) Judgements of and by Representativeness in Kahneman, D., Slovic, P., & Tversky, A. *Judgment under uncertainty: heuristics and biases*. Cambridge, Cambridge University Press.

Kahneman, D. & Tversky, A. (1974) Availability: A heuristic for judging frequency and probability in Kahneman, D., Slovic, P., & Tversky, A. *Judgment under uncertainty: heuristics and biases*. Cambridge, Cambridge University Press.

Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. *American Psychologist*, 39(4), 341-350.

Kahneman, D. (2013). *Thinking, Fast and Slow*. London, Penguin Books.

Matsakis, L. (2019) <https://www.wired.com/story/wired-guide-personal-data-collection/> (accessed 30052021)

Melendez, S. and Pasternack, A. (2019) <https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information> (accessed 30052021)

Oswald, M. & Grosjean, S.(2004), "Confirmation bias", in Pohl, Rüdiger F. (ed.), *Cognitive illusions: A handbook on fallacies and biases in thinking, judgement and memory*, Hove, Psychology Press.

Shotton, R. (2018). *The Choice Factory: 25 behavioural biases that influence what we buy*. Hampshire, Harriman House.

Taleb, N. (2007) *The Black Swan*. New York, Random House.

Taleb N. (2018) *Skin in the Game: Hidden Asymmetries in Daily Life*. New York, Random House.

Thaler, R. & Sunstein, C. (2008). *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press.

About the authors



Araba Cole

Global Director, Safety & Security at the International Rescue Committee

Araba Cole is a security professional with a broad range of skills, interests, and experiences, including an undergraduate degree in archaeology, an operational tour with the British Army, and security roles with international humanitarian and development organisations such as INSO, NRC, and the World Bank. She has spent her career in some of the most vibrant and dynamic places in the world, including DR Congo, Afghanistan, Libya, and Ethiopia, and now works on creative, insightful, and delivery-orientated approaches to security risk management and operational resilience.



Panagiotis Olympiou

Risk and Public Policy Consultant

Panagiotis Olympiou is a conflict and risk management expert who focuses on improving risk analysis and decision-making practices for public and private organisations. He has worked on Third Party Monitoring in Libya with Altai Consulting; on Site Management (CCCM) with DRC in Greece, where he chaired the National Site Management Support Working Group; and served as a Safety Advisor with INSO in Afghanistan. Panagiotis holds an MA in Conflict Management & International Economics from Johns Hopkins University's School of Advanced International Studies (SAIS), and a BA in Political Science from the Aristotle University of Thessaloniki. He is a Second Lieutenant in Reserve of the Hellenic Army.