Economics–driven behaviour intervention support in organizations

Albesë Demjaha[1†], Simon Parkin[2†], and David Pym[1]

[1] University College London and Alan Turing Institute, UK
[2] University College London, UK
{*albese.demjaha.16, s.parkin, d.pym*}*@ucl.ac.uk*

1 Introduction

Security policies may dictate specific *security-related behaviours* which employees are expected to adopt. There are challenges in guaranteeing that behaviours are changed successfully [9]. Declaring a behaviour in a security policy is not an assurance that the behaviour will happen. Employees may not see how policy applies to them, find it difficult to follow, or regard policy expectations as unrealistic [6]. Security managers must have a strategy for how to provision for security, provide workable policy, and support user needs. The strategy includes knowing which data to collect, and a capability to anticipate the effects of provisioning decisions.

We present a framework [4], built on a consolidation of traditional and behavioural economics principles, with the goal: to *Better support for 'good enough' security-related decisions, by individuals within an organization, that best approximate secure behaviours under constraints, such as limited time or knowledge.* This requires us to identify the factors affecting security behaviours, where these should be considered by an organization to inform policy design. Within this is a need to support the identification of provisioning requirements, and describe expectations of users.

2 Applying economics to organizational security

In traditional economics, a decision-making structure assumes a rational agent [10]. A rational agent has the capabilities and resources to make the decision which will be most beneficial for them. The agent knows all possible choices, and is assumed to have complete information when evaluating those choices, as well as a detailed analysis of probability, costs, gains, and losses [10].

Behavioural economics refers to the concept of *bounded rationality*, where an agent's rationality is bounded due to cognitive limitations and time restrictions. The bounded agent turns instead to 'rules of thumb' and makes ad hoc decisions based on a quick evaluation of *perceived* probability, costs, gains, and losses [5, 10].

† Authors contributed equally.

Table 1 outlines the differences between the decision-making process of a rational agent and a bounded agent. Given the increasing adoption of behaviour change programmes for security, it is by considering these principles that we explore more constructive decision-support in organizations.

Research has advocated *influencing* security and privacy behaviours through the application of *nudge theory* (e.g., [1]). Redmiles et al. [8] effectively advocate for identifying and presenting options which are optimal for the decision-maker. Morisset et al. [7] present a model of 'soft enforcement', where the influencer (security function) edits the choices available to a decision-maker (employees) toward removing bad choices. We explore where there are 'gaps' in capabilities, and where the range of behaviour choices is in effect a negotiation between the two parties.

Table 1. Rationality vs. bounded rationality in decision-making.

Traditional economics	*Behavioural economics*
RATIONAL AGENT	**BOUNDED AGENT**
- detailed evaluation of costs, gains, and losses - complete information - careful calculation of potential investment ↓ chosen outcome ↓ optimal decision	- brief consideration of perceived costs, gains, and losses - incomplete information - insufficient skills, knowledge, or time - quick evaluation of risks driven by loss aversion ↓ decision fatigue ↓ satisfactory decision

3 A framework for security choices

We advocate support for *bounded security decision-making*. This also acts to distance this approach from any ambiguous conflation of concepts from traditional and behavioural economics. Specifically, we wish to avoid the existing tendency to apply behavioural intervention concepts to security while planning interventions in a way that implies a rational agent.

We adapt the security investment model developed by Caulfield and Pym [3], towards supporting the decision-maker to choose 'good enough' behaviours under constraints on knowledge and resources. The focal point in this model is the decision-point of the agent (the decision-maker), incorporating elements of the decision-making process which inform the decision. It is here where we reconcile elements of behavioural economics, and the limited awareness of available choices provided by the organization (the influencer).

Fig. 1. A decision point in a decision-maker's process *bounded security decision-making* (adapting elements from Caulfield and Pym [3]).

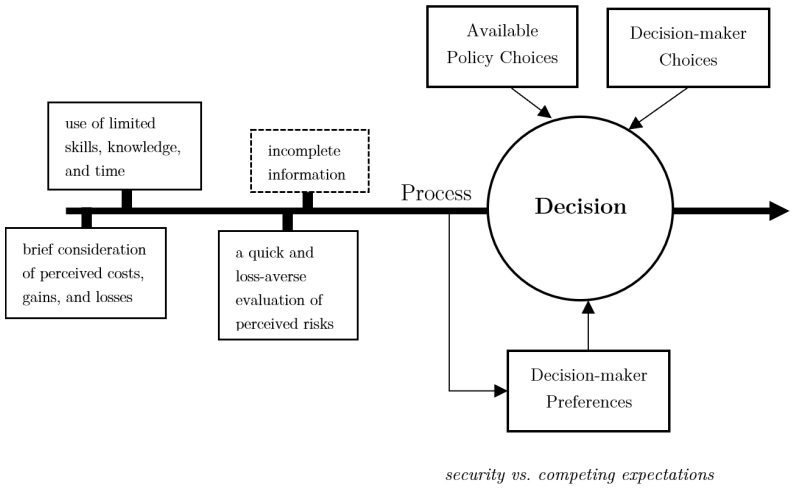


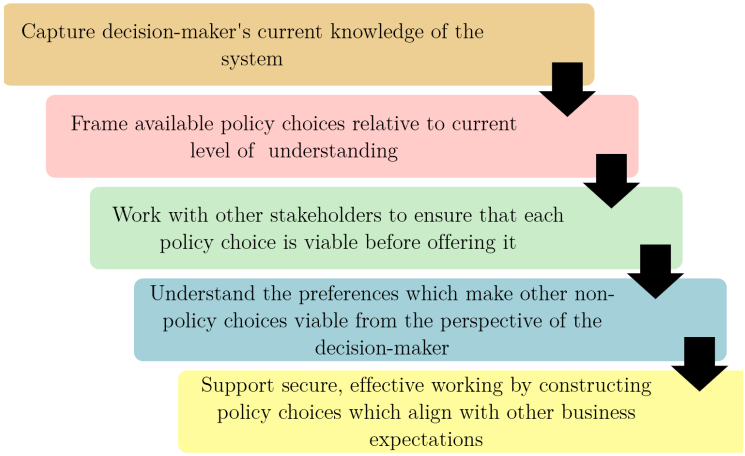
Figure 1 illustrates the components and processes to consider at policy design. *Influencer* refers to the security policy-maker in the organization, and *decision-maker* (DM) the bounded agent (the employee). There is an interplay between Process, Decision-maker preferences, alongside choices and decisions. The framework would be instantiated as in Figure 2.

4 Future directions

To inform building of secure, effective policy choices (as in Figure 2, **security modelling** can begin to forecast the impact of specific investment decisions by the influencer. Information that represents employees' perspectives of security should be incorporated into agent-based models configured according to the principles of bounded security decision-making. This will inform the viability of new controls.

Models have the potential to support regular improvements to security behaviour support. This can include monitoring of **security diets**, wherein the perceived occurrence and costs of regular security behaviours are documented (for instance where they occur in a typical working day). These costs can then be considered against other expectations and policies from elsewhere in the organization. Combinations of distinct behaviour choices can also be defined and considered by both sides in negotiating a solution for security **policy concordance** [2], leveraging the co-developed choice architecture.

Fig. 2. Framework components map to model and data-gathering components.



References

1. Acquisti, A.: Nudging privacy: The behavioral economics of personal information. IEEE security & privacy **7**(6) (2009)
2. Ashenden, D., Lawrence, D.: Security dialogues: Building better relationships between security and business. IEEE Security & Privacy **14**(3), 82–87 (2016)
3. Caulfield, T., Pym, D.: Improving security policy decisions with models. IEEE Security & Privacy **13**(5), 34–41 (2015)
4. Demjaha, A., Parkin, S., Pym, D.: You've left me no choices: Security economics to inform behaviour intervention support in organizations. In: Socio-Technical Aspects of Security and Trust (STAST'19). Springer (2019)
5. Johnson, E.J., Shu, S.B., Dellaert, B.G., Fox, C., Goldstein, D.G., Häubl, G., Larrick, R.P., Payne, J.W., Peters, E., Schkade, D., et al.: Beyond nudges: Tools of a choice architecture. Marketing Letters **23**(2), 487–504 (2012)
6. Kirlappos, I., Parkin, S., Sasse, M.A.: Learning from "shadow security": Why understanding non-compliance provides the basis for effective security. In: Workshop on Usable Security (USEC) 2014 (2014)
7. Morisset, C., Yevseyeva, I., Groß, T., van Moorsel, A.: A formal model for soft enforcement: influencing the decision-maker. In: International Workshop on Security and Trust Management. pp. 113–128. Springer (2014)
8. Redmiles, E.M., Mazurek, M.L., Dickerson, J.P.: Dancing pigs or externalities?: Measuring the rationality of security decisions. In: Proceedings of the 2018 ACM Conference on Economics and Computation. pp. 215–232. ACM (2018)
9. Renaud, K., Zimmermann, V.: Ethical guidelines for nudging in information security & privacy. International Journal of Human-Computer Studies **120**, 22–35 (2018)
10. Simon, H.A.: Rational choice and the structure of the environment. Psychological review **63**(2), 129 (1956)