Name of theory
COM-B Model

Key reference
(Michie et al., 2011)

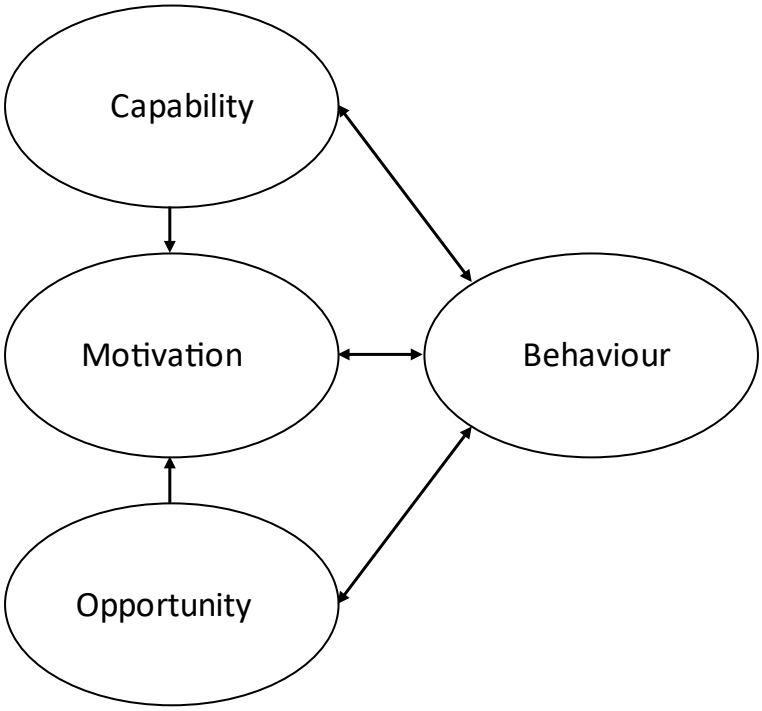

Figure 1. The COM-B Model.

Description
The COM-B model explain determinants of behaviour and is an acronym for the four factors it contains: Capability, Opportunity, and Motivation as the three predictors that lead to Behaviour. Each of the three predictors can be further broken down into two separate factors: physical and psychological capability, physical and social opportunity, and conscious and unconscious motivation.

Capability refers to whether a person both **physically** (in the case of movement) and **psychologically** (cognitive skills) able to perform the behaviour. For instance, knowing how to recognise a phishing email would be part of someone's psychological capability to report potential phishing emails. Whether or not someone has the **opportunity** to act depends on the situational factors in which they are operating. The **physical opportunity** to plug in a USB drive can for instance be restricted by the IT department removing the USB-sockets on workstations. This would reduce the risk of someone (accidentally) installing malware using non-secured USB-devices. The **social opportunity** refers to the influence of someone's social circle. If they are showing an interest in cybersecurity, or think that cybersecurity is important, this affects the people around them. The third predictor, **motivation** again has two levels: conscious and unconscious motivation. **Conscious motivation** consists of the beliefs and intentions of individuals towards the target behaviour (e.g., believing it is important to secure patient or customer data), whereas the **unconscious motivation** contains emotions and

habits (e.g. the habit to check who you're sending emails to, to ensure that you don't accidentally leak confidential data through an attachment). Capability and opportunity influence the motivation of individuals, and all three predictors (Capability, Opportunity, and Motivation) influence behaviour.

Application within the field of cybersecurity

The COM-B model is somewhat used in cybersecurity. The attractiveness of this model seems to relate to the use of criminological theories in cybercrime research, as the three predictors (capability, opportunity, and motivation) are typically factors considered when trying to identify culprits after a specific crime. More elaborative research on the predictive value for cybersecurity behaviours, and the use of the COM-B model to inform cybersecurity training is needed.

Annotated bibliography

Alshaikh et al. (2019). In this paper, the authors map a range of factors relating to cybersecurity behaviour on the COM-B model, to explore the requirements of information security education, training, and awareness (SETA) programs. They suggest a more theoretical approach to the development of these SETA programs and use the Behavioural Change Wheel which incorporates the COM-B model as a proof of concept.

Van der Kleij et al. (2020). This paper reports a study on the predictive power of the COM-B model for a specific cybersecurity behaviour: Data leakage prevention by bank employees. The study shows that the COM-B model can be used to predict this form of behaviour, and that capability is an important factor in data leak prevention behaviour.

Van der Kleij et al. (2021). This paper reports on a wider study on the predictive power of the COM-B model, assessing its power to predict the cybersecurity behaviour of citizens. While the COM-B model predicted cybersecurity behaviours, opportunity was not as relevant as the other two factors (motivation and capability).

References

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: an approach for cyber security education training and awareness. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden, June 8-14, 2019.

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*. https://doi.org/10.1186/1748-5908-6-42

van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Computers & Security*, *97*, 101970.

van der Kleij, R., van't Hoff-De Goede, S., Weijer, S. V. D., & Leukfeldt, R. (2021). How Safely Do We Behave Online? An Explanatory Study into the Cybersecurity Behaviors of Dutch Citizens. In *International Conference on Applied Human Factors and Ergonomics* (pp. 238-246). Springer, Cham.