Name of theory
Operant conditioning

Description
Operant conditioning is a method of learning where behaviours are shaped based on reinforcements and punishments. These reinforcements and punishments come in positive and negative forms. A positive reinforcement means that someone gains something they would want by performing the behaviour, such as a treat. A negative reinforcement consists of an unwanted stimulus to be removed from the situation. A positive punishment is when someone is actively punished for their behaviour, such as a fine when caught speeding on the motor way. A negative punishment is taking away a positive stimulus, for example limiting someone's freedom to choose an alternative or freedom of movement. People are said to learn through these forms of reinforcement and punishment which behaviours are socially acceptable, and which result in higher gains, or losses. By receiving these forms of feedback, people can adjust their behaviour accordingly. For the punishments and reinforcements to be most effective, they should be administered as soon as possible after the behaviour has been performed. B.F. Skinner made this topic famous, using his own device called a Skinner box to run tests on operant conditioning in animals. At the end of this document, you can find a video of an experiment with a Skinner box for doves.

Application within the field of cybersecurity
In the field of cybersecurity, many end-users in organisations do not know which behaviours will lead to positive or negative outcomes. Therefore, end-users often use a 'trial and error' approach, where they test security policies and guidelines by doing what they think is best. If an organisation has good monitoring abilities for their systems, any unwanted behaviours should be quickly detected and adjusted. However, with the vast array of options that end-users have at their disposal, it can be difficult to track each unwanted cybersecurity behaviour. As a result, end-users learn that their insecure behaviours are not met with any serious consequences, and as a result keep performing these behaviours. If performing these behaviours then also leads to negative reinforcement (for example because the insecure behaviour reduces bureaucracy and thereby stimulates productivity), not only is a punishment lacking, but in fact, people are encouraged to perform the unwanted behaviour more often.

A second application of operant conditioning in the field of cybersecurity is that traditionally, companies have seen cybersecurity policies as strictly enforced policies, where people should be punished if they do not adhere to them. More recently, some organisations have been moving towards training and supporting end-users, as they realise that if they always punish when something goes wrong (e.g., when someone clicks on a dubious URL in an phishing test), people are less likely to come forward when a cyber incident takes place. The focus in cybersecurity will therefore lie more on the reinforcement side, than the punishment side, as punishing employees might lead to reduced reporting behaviour.

Annotated bibliography

Yang and Johnston (2019). The authors argue for the use of gains and rewards instead of punishments in motivating employees to act more cybersecure in the day-to-day tasks. They propose an experiment to test the effectiveness of framing adherence to Information Security Policies (ISPs) as a gain rather than as a potential punishment in case people do not adhere to these policies. The paper does not report the results of the proposed study.

Yeoh et al. (2021). Yeoh and colleagues suggest that employees who are subjected to a phishing awareness campaign could benefit from these campaigns if they incorporate operant conditioning principles. The authors conducted a case study of a large phishing awareness campaign and find that the learning process that end-users go through can be seen as operant conditioning, and that applying these principles correctly could lead to improved phishing awareness.

References

Yang, N.V., & Johnston, A.C. (2019). The Application of Operant Conditioning Theory in Employees' IS Security Behavioral Management. *ICIS*.

Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2022). Simulated phishing attack and embedded training campaign. Journal of Computer Information Systems, 62(4), 802-821.

Video

Dove in a Skinner box
https://www.youtube.com/watch?v=CtoH5tlr-bI

A video to demonstrate research on operant conditioning using a Skinner box for doves.