GUIDANCE

Title: A Guide to Developing a Cybersecurity Strategy Using Behavioural Science

Date: 30th April 2024

Cybersecurity is not just about technology; it is also about the people who use it. Understanding and influencing human behaviour is essential to enhancing cybersecurity measures. The COM-B model, which stands for Capability, Opportunity, and Motivation, provides a robust framework for applying behavioural science to cybersecurity strategy development. This guide will walk you through the steps of using the COM-B model to craft a cybersecurity strategy that addresses both technological and human factors.

Step 1: Assess Current Security Behaviours

Data Collection

Begin by gathering data on your organisation's current cybersecurity behaviours. This can be achieved through:

- Surveys and interviews to understand employee attitudes and knowledge about cybersecurity.
- Observational studies to see how policies are practically followed.
- Incident reports to identify common security failures and their contexts.

Analysis

Analyse the data to identify problematic behaviours that need to be changed. For example, if many employees are clicking links on phishing emails, this behaviour needs to be addressed.

Step 2: Apply the COM-B Model

Capability

Determine if employees have the necessary knowledge and skills to perform secure behaviours. Questions to consider:

- Do employees know how to recognise a phishing email?
- Are they aware of the organisation’s security protocols?

Opportunity

Examine the external factors that make it possible or prompt the desired behaviour. Consider:

- Are there sufficient resources and tools available to employees for secure behaviour?
- Do current work processes and environments support or hinder secure practices?

Motivation

Understand the psychological factors driving behaviours, which can be reflective (thoughtful decisions) or automatic (habits). Reflect on:

- What incentives exist for employees to follow security protocols?
- Are there any disincentives for insecure behaviour, such as penalties or negative feedback?

Step 3: Identify Intervention Functions

Based on the insights from the COM-B analysis, select appropriate intervention functions to change behaviours. These might include:

- **Education** to enhance capability by increasing understanding and skills.
- **Persuasion** to increase motivation through communication that promotes emotional engagement.
- **Incentivisation** to create expectation of reward for secure behaviour.
- **Coercion** to create expectation of punishment or cost for non-compliance.
- **Training** to build physical skills or rehearse the behaviours.

Step 4: Implement Supporting Policies

Choose policies that will support the interventions. Options include:

- **Guidelines**: Developing clear, accessible, and concise security policies.
- **Communication/marketing**: Using internal communications to promote security awareness and changes.
- **Environmental/social planning**: Organising the physical or digital environment to reduce barriers and enhance opportunities for secure behaviour.
- **Regulation**: Implementing rules that mandate secure behaviours.

Step 5: Develop and Deploy the Strategy

Integration

Integrate the chosen interventions and policies into a comprehensive cybersecurity strategy. Ensure that the strategy is holistic, addressing all identified behaviours through multiple interventions.

Implementation

Roll out the strategy across the organisation. This may involve:

- Conducting training sessions.
- Launching a communication campaign.
- Updating or deploying new security software tools.
- Revising work processes to support secure behaviours.

Step 6: Evaluate and Adapt

Monitoring

Regularly monitor the effectiveness of the strategy through ongoing assessments and audits. Pay attention to both compliance rates and incident reports.

Feedback

Collect feedback from employees about the strategy's impact and any barriers they face in complying with the security behaviours.

Adaptation

Based on the feedback and monitoring results, make necessary adjustments to the strategy to improve its effectiveness and address any new security challenges.

Conclusion

Developing a cybersecurity strategy that integrates behavioural science and employs the COM-B model offers a multidimensional approach that transcends conventional security measures. By focusing on Capability, Opportunity, and Motivation, organisations can craft strategies that are not only comprehensive but also deeply embedded in the understanding of human behaviour. This enables a nuanced approach to cybersecurity, where technological defences are complemented by behavioural interventions designed to influence employee actions positively.

The application of the COM-B model facilitates a more dynamic and adaptable cybersecurity strategy. It allows organisations to not just respond to existing threats but to anticipate potential behavioural vulnerabilities before they become exploitable. By continuously assessing and modifying the strategy based on actual employee behaviour and feedback, the organisation can maintain a robust security posture that evolves with both technological advancements and changes in workforce dynamics.

Moreover, this human-centred approach fosters a culture of security that permeates all levels of the organisation. When employees understand the role they play in cybersecurity and are equipped, motivated, and allowed to act securely, they transform from the weakest link in the security chain into its strongest defenders. This cultural shift is vital for the long-term resilience of the organisation's cybersecurity efforts.