Beyond the Firewall

WHITE PAPER

Title: Implementing the Behaviour Change Wheel for Enhanced Cybersecurity Strategies

Date: May 20th, 2024

Author: Andy Wood

Abstract:

This white paper explores the application of the Behaviour Change Wheel (BCW), a systematic approach to understanding and influencing behaviour change, in the context of cybersecurity. By leveraging this framework, organisations can enhance their cybersecurity strategies, improving cultural maturity and resilience against cyber threats.

Introduction

In the landscape of cybersecurity, human factors play a critical role in the effectiveness of security measures. Despite robust technological defences, human error remains a significant vulnerability, often exploited by cybercriminals through tactics such as phishing, social engineering, and insider threats. The importance of addressing these human elements alongside technological solutions cannot be overstated. The Behaviour Change Wheel (BCW), developed by Michie, van Stralen, and West (2011), provides a comprehensive model for understanding and changing behaviour in various contexts, initially focusing on health. Its principles and frameworks, however, have profound potential applications in cybersecurity. By leveraging the BCW, organisations can design and implement strategies that go beyond technical solutions to foster a resilient security culture. This paper discusses how the BCW can be adapted to develop a holistic cybersecurity strategy that emphasises the interplay between human behaviour and technological measures, thereby enhancing overall security posture and reducing vulnerabilities stemming from human factors.

The Behaviour Change Wheel (BCW) Framework

The BCW is a comprehensive framework developed to guide the design and implementation of behaviour change interventions. It integrates various theories of behavioural change into a cohesive model. The BCW comprises **three layers**: the hub (the behaviour system), the middle layer (intervention functions), and the outer layer (policy categories). See Figure 1 below.

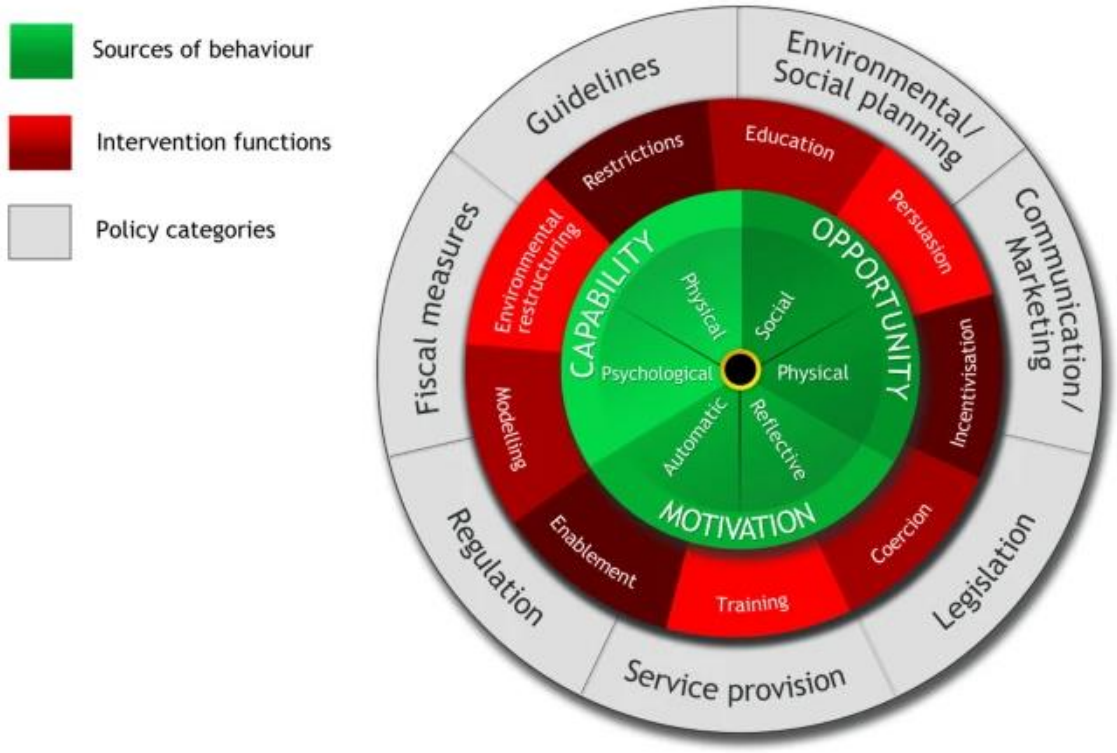

Figure 1: ***The Behaviour Change Wheel*** *(source: Michie, S. et al (2011)*

<u>Sources of Behaviour</u>

Sources of behaviour are represented in the central hub of the model, which outlines a comprehensive understanding of what drives behaviour. The BCW identifies three core components that interact to produce behaviour: Capability, Opportunity, and Motivation. This model is often referred to as the COM-B system[1].

[1] Beyond the Firewall have a published whitepaper on COM-B available here: https://buildasecurityculture.com/wp-content/uploads/2024/05/utilizing-the-com-b-model-for-cultural-maturity-in-cybersecurity.pdf

Here's a detailed description of each component:

1. **Capability**:
    - **Physical Capability**: In cybersecurity, this may be less relevant, but it could involve having the necessary physical devices or tools to perform security tasks (e.g., a secure computer or smartphone).
    - **Psychological Capability**: This is critical in cybersecurity and includes knowledge and understanding of security protocols, awareness of threats, and the ability to recognise phishing attempts or understand the importance of strong passwords. Training programs, educational workshops, and informational resources can enhance psychological capability.
2. **Opportunity**:
    - **Physical Opportunity**: This includes the external factors that facilitate secure behaviour, such as the availability of security tools (e.g., firewalls, antivirus software, password managers) and organisational policies that mandate certain behaviours (e.g., mandatory use of two-factor authentication). It also involves providing easy access to these tools and ensuring they are user-friendly.
    - **Social Opportunity**: This involves the social environment and cultural norms within an organisation or community. Encouraging a culture of cybersecurity, where peers and leaders model and promote secure behaviour, can enhance social opportunity. For example, regular discussions about cybersecurity in team meetings and visible support from leadership can promote a security-conscious culture.
3. **Motivation**:
    - **Reflective Motivation**: This includes the conscious intentions and beliefs about cybersecurity. For instance, an employee's belief in the importance of following security protocols to protect company data can drive secure behaviour. Interventions might include training that highlights the consequences of security breaches and the benefits of maintaining strong cybersecurity practices.
    - **Automatic Motivation**: This involves habits and emotional responses. Developing automatic behaviours such as routinely locking screens, regularly updating passwords, and immediately reporting suspicious activities can be crucial. Gamification, rewards, and recognition for secure behaviours can help reinforce these habits.

The COM-B system highlights how these three components interact dynamically to influence behaviour. For example:

- **Capability** can affect **Motivation**: If someone lacks the skills or knowledge to perform a behaviour, they may not be motivated to try.
- **Opportunity** can affect **Capability**: Having access to training programs or resources can enhance a person's physical or psychological capability.
- **Motivation** can affect **Opportunity**: A motivated individual might seek out or create opportunities to engage in a desired behaviour.

By understanding and addressing these sources of behaviour, interventions can be more effectively designed to target the specific barriers and facilitators relevant to the behaviour in question. The BCW uses this framework to guide the selection of intervention functions and policy categories that are likely to be effective in achieving behaviour change.

Intervention Functions

Intervention functions refer to specific strategies or actions designed to influence and improve cybersecurity behaviours among individuals within an organisation. These functions are part of a systematic approach to behaviour change, guided by the BCW, which ensures that interventions are targeted, effective, and comprehensive. Here's how each of the 9 intervention functions can be applied to cybersecurity:

1. **Education**:
    - **Application**: Increasing knowledge and understanding about cybersecurity threats and best practices. Educational efforts can inform employees about the importance of strong passwords, recognising phishing emails, and safe internet use.
    - **Example**: Conducting workshops, webinars, and distributing informational materials to educate staff on identifying and avoiding common cyber threats.
2. **Persuasion**:
    - **Application**: Using communication to shape attitudes and motivate secure behaviours. Persuasion techniques can create positive attitudes towards cybersecurity practices and highlight the benefits of compliance.
    - **Example**: Running campaigns that use compelling messages and testimonials to stress the importance of following security protocols, such as stories of how secure behaviours have prevented breaches.

3. **Incentivisation**:
    - **Application**: Creating incentives to encourage secure behaviour. Rewards and recognition can motivate employees to adhere to security practices.
    - **Example**: Offering bonuses, recognition awards, or other incentives for employees who demonstrate exceptional adherence to cybersecurity policies.
4. **Coercion**:
    - **Application**: Implementing measures that create consequences for non-compliance with security protocols. This function ensures that there are clear, negative repercussions for failing to follow security practices.
    - **Example**: Establishing penalties, such as disciplinary action or loss of privileges, for employees who repeatedly violate cybersecurity policies.
5. **Training**:
    - **Application**: Providing training to develop the skills necessary for secure behaviour. Training sessions can help employees recognise and respond appropriately to cyber threats.
    - **Example**: Conduct regular, hands-on training sessions that simulate cyber-attacks, such as phishing simulations, to improve employees' practical skills.
6. **Restriction**:
    - **Application**: Implementing policies and technical controls that limit opportunities for insecure behaviour. Restrictions help ensure that secure behaviour is the default and easiest option.
    - **Example**: Enforcing strict access controls, using software that limits the ability to download unauthorised applications, and requiring multi-factor authentication for system access.
7. **Environmental Restructuring**:
    - **Application**: Changing the physical or digital environment to promote secure behaviour. Modifications in the work environment can support and encourage adherence to security protocols.
    - **Example**: Setting up workstations with privacy screens, creating secure areas for handling sensitive information, and organising the digital workspace to minimise the risk of data leaks.

8. **Modelling**:
    - **Application**: Demonstrating secure behaviour through role models and influential figures within the organisation. Employees are more likely to adopt secure practices if they see them modelled by their peers and leaders.
    - **Example**: Leaders and managers visibly following and promoting security protocols, such as always using secure passwords and regularly updating their software.
9. **Enablement**:
    - **Application**: Providing support and resources to make secure behaviour easier and more achievable. Enablement removes barriers to secure behaviour and provides tools that facilitate compliance.
    - **Example**: Offering user-friendly password managers, providing 24/7 IT support for security issues, and ensuring employees have access to necessary cybersecurity tools and resources.

These intervention functions can be used individually or in combination to create comprehensive behaviour change interventions tailored to specific populations and contexts. By addressing different aspects of the behaviour change process, the BCW helps ensure that interventions are systematic, theory-based, and effective. The intervention functions are implemented through policy, which we will explore next.

Policy Categories

The outer layer of the BCW comprises policy categories that support the implementation of intervention functions. In the context of cybersecurity, these policy categories guide the development of overarching strategies and frameworks to promote secure behaviours. Below is a description of each policy category and how it can be applied to cybersecurity.

1. **Communication/Marketing**:
    - **Application**: Use targeted communication and marketing campaigns to raise awareness about cybersecurity threats and best practices. This could include regular newsletters, email alerts about new threats, social media campaigns, and informational posters in the workplace.
    - **Example**: Launching a "Cybersecurity Awareness Month" campaign to educate employees about phishing, password security, and safe internet use.

2. **Guidelines**:
    - **Application**: Develop and disseminate clear guidelines and protocols for cybersecurity. These should detail the procedures for handling sensitive information, reporting incidents, and maintaining secure systems.
    - **Example**: Creating a comprehensive cybersecurity handbook that outlines the steps for creating strong passwords, using encryption, and recognising phishing emails.
3. **Fiscal Measures**:
    - **Application**: Allocate financial resources to support cybersecurity initiatives, such as investing in advanced security technologies, funding training programs, and providing incentives for secure behaviour.
    - **Example**: Offering financial bonuses to departments that achieve specific cybersecurity goals, such as zero security breaches in a quarter.
4. **Regulation**:
    - **Application**: Implement regulatory measures that mandate certain cybersecurity practices. This can include internal policies as well as adherence to external regulations and standards (e.g., GDPR, HIPAA).
    - **Example**: Requiring all employees to complete annual cybersecurity training and adhere to industry standards for data protection.
5. **Legislation**:
    - **Application**: Enforce laws and legal requirements related to cybersecurity. This includes compliance with national and international legislation that governs data protection and cybersecurity practices.
    - **Example**: Ensuring company policies comply with the General Data Protection Regulation (GDPR) to protect customer data.
6. **Environmental/Social Planning**:
    - **Application**: Design and restructure the organisational environment to support secure behaviours. This can involve both physical and social aspects, such as creating a culture of security and providing the necessary tools and resources.
    - **Example**: Designing office spaces that encourage secure behaviours, like privacy screens on computers and secure areas for handling sensitive information.

7. **Service Provision**:
    - **Application**: Offer services that support cybersecurity efforts. This includes providing IT support, access to security tools, and ongoing training and development opportunities.
    - **Example**: Setting up a dedicated cybersecurity helpdesk to assist employees with security issues and questions.
8. **Training**:
    - **Application**: Develop and implement training programs to enhance cybersecurity skills and knowledge. Training should be continuous and adapted to the evolving threat landscape.
    - **Example**: Conduct regular cybersecurity workshops, webinars, and simulated phishing exercises to keep employees updated on the latest threats and defence strategies.
9. **Enablement**:
    - **Application**: Facilitate the adoption of secure behaviours by removing barriers and providing support. This includes making it easier for employees to follow security protocols and access necessary resources.
    - **Example**: Providing user-friendly password managers, single sign-on systems, and automated security updates to reduce the burden on employees.

By strategically applying these policy categories, organisations can create a supportive framework that encourages and sustains secure cybersecurity behaviours among employees.

Case Studies and Outcomes

Below are three case studies that describe three ways of applying elements of the BCW framework to address different cyber threats.

Case Study 1: Global Financial Services Firm

Background: A major financial services organisation faced recurring issues with data breaches due to phishing attacks. An initial assessment using the COM-B model revealed that while employees had the capability and opportunity to recognize phishing attempts (through prior training and available security software), their motivation to consistently apply this knowledge was lacking.

Intervention: The organisation decided to employ the 'Incentivization' and 'Persuasion' functions of the BCW. They introduced a reward system where departments demonstrating exemplary cybersecurity behaviours, such as reporting suspicious emails, were publicly recognized and financially rewarded.

Outcome: Within six months, the organisation saw a 45% increase in reported incidents of phishing attempts, suggesting heightened vigilance. Furthermore, follow-up surveys indicated a significant boost in employee motivation and engagement with cybersecurity protocols.

Case Study 2: Large Healthcare Provider

Background: A large healthcare provider struggled with securing patient data across its numerous service locations. The BCW was utilized to analyse the behaviour surrounding data security practices among staff. The analysis identified significant gaps in both 'Capability' and 'Opportunity.'

Intervention: To address these gaps, the healthcare provider implemented two key interventions. First, under 'Education,' they developed targeted training sessions to enhance staff understanding and capability in handling sensitive information. Second, they improved 'Environmental restructuring' by upgrading their electronic health records system to include automatic logging of data access and more user-friendly security features to reduce barriers to secure behaviour.

Outcome: Post-intervention, the organization reported a 30% reduction in incidental data breaches and unauthorized data access instances. Employee feedback highlighted easier data management processes and increased awareness of data security importance.

Case Study 3: International E-commerce Corporation

Background: This e-commerce giant identified a pattern of weak password practices among its global workforce, leading to increased vulnerability to account breaches. A detailed COM-B analysis indicated that while employees understood the importance of strong passwords ('Capability'), they did not feel personally at risk ('Motivation'), nor did they find the process of updating their passwords convenient ('Opportunity').

Intervention: The corporation employed 'Enablement' by introducing a password management tool that facilitated the creation and storage of complex passwords without memorisation. Additionally, 'Persuasion' was used via an internal marketing campaign that shared real stories of individuals impacted by weak security practices, personalising the risk.

Outcome: The adoption of the password management tool reached 80% of the workforce within three months, and the frequency of password-related breaches decreased significantly. The storytelling approach helped shift employees' perceptions of risk, making the threat more real and immediate.

Applying BCW in Developing a Cybersecurity Strategy

Applying the BCW to a cybersecurity strategy involves a systematic approach. Below is a step-by-step guide on how to apply the BCW to develop a comprehensive cybersecurity strategy.

Step 1: Understand the Problem

Identify the Target Behaviours

- Determine which specific behaviours need to change to enhance cybersecurity. Examples include creating strong passwords, recognising phishing emails, regularly updating software, and reporting suspicious activities.

Assess the Current Situation

- Conduct a thorough assessment of the current cybersecurity landscape within the organisation. This includes understanding existing behaviours, identifying vulnerabilities, and recognising areas where human error frequently occurs.

Step 2: Analyse the Behaviour Using the COM-B Model

Capability

- **Physical Capability**: Assess whether employees have the necessary physical tools and resources (e.g., secure devices, software).
- **Psychological Capability**: Evaluate employees' knowledge and skills related to cybersecurity. Identify gaps in understanding or misconceptions about secure behaviours.

Opportunity

- **Physical Opportunity**: Examine the physical environment to ensure it supports secure behaviours. Ensure that employees have access to necessary security tools and resources.
- **Social Opportunity**: Analyse the social environment and cultural norms within the organization. Determine whether there is a supportive culture for cybersecurity and peer influence that encourages secure behaviour.

Motivation

- **Reflective Motivation**: Understand the conscious motivations behind employees' actions. This includes their beliefs about the importance of cybersecurity and their intentions to follow security protocols.
- **Automatic Motivation**: Identify habits and automatic responses related to cybersecurity. Assess whether there are ingrained behaviours that either support or undermine security efforts.

Step 3: Identify Appropriate Intervention Functions

Using the insights gained from the COM-B analysis, select the most relevant intervention functions from the BCW to address identified issues:

1. **Education**: Develop training programs to improve cybersecurity knowledge.
2. **Persuasion**: Create campaigns to positively influence attitudes towards cybersecurity.
3. **Incentivization**: Implement rewards for secure behaviours.
4. **Coercion**: Establish consequences for non-compliance with security protocols.
5. **Training**: Offer practical, hands-on training to build necessary skills.
6. **Restriction**: Enforce policies that limit opportunities for insecure behaviour.
7. **Environmental Restructuring**: Modify the environment to make secure behaviours easier.
8. **Modelling**: Use role models to demonstrate secure behaviours.
9. **Enablement**: Provide resources and support to facilitate secure behaviours.

Step 4: Develop a Comprehensive Cybersecurity Strategy

Design Interventions

- Based on the selected intervention functions, design specific interventions that will be implemented. This may include educational programs, communication campaigns, new policies, and changes to the physical environment.

Plan Implementation

- Create a detailed plan for implementing the interventions. This should include timelines, responsible parties, necessary resources, and methods for measuring progress and effectiveness.

Step 5: Implement the Strategy

Roll Out Interventions

- Begin implementing the interventions according to the plan. Ensure that all employees are aware of the new initiatives and understand their roles in improving cybersecurity.

Monitor and Adjust

- Continuously monitor the effectiveness of the interventions. Collect data on behaviour changes, security incidents, and feedback from employees. Adjust the strategy as needed to address any emerging issues or challenges.

Step 6: Evaluate and Sustain

Evaluate Outcomes

- Conduct a thorough evaluation of the strategy's impact on cybersecurity behaviours and overall security posture. Use both quantitative (e.g., reduction in security incidents) and qualitative (e.g., employee feedback) measures.

Sustain Improvements

- Ensure that successful interventions are sustained over time. This may involve integrating cybersecurity practices into regular training, updating policies as needed, and maintaining a culture that prioritizes security.

Example: Application of BCW to Phishing Awareness

1. **Understand the Problem**: Employees frequently fall for phishing emails.
2. **Analyse the Behaviour**:
    - **Capability**: Many employees lack the skills to identify phishing attempts.
    - **Opportunity**: Emails are not adequately filtered, and there is a lack of clear reporting mechanisms.
    - **Motivation**: Employees do not see the immediate consequences of phishing attacks.
3. **Identify Intervention Functions**: Education, Training, Environmental Restructuring, and Enablement.
4. **Develop the Strategy**:
    - **Education**: Launch a campaign to educate employees on recognising phishing emails.
    - **Training**: Conduct simulated phishing exercises and provide feedback.
    - **Environmental Restructuring**: Implement better email filtering and create an easy-to-use reporting system.
    - **Enablement**: Provide tools like email verification software.
5. **Implement the Strategy**: Roll out the educational campaign, start training sessions, enhance email systems, and distribute verification tools.
6. **Evaluate and Sustain**: Monitor the rate of phishing incidents, gather feedback, and adjust the interventions as needed to ensure long-term success.

By following these steps, organisations can effectively apply the BCW to develop a robust cybersecurity strategy that addresses both human and technological aspects of security.

Conclusion

The illustrative case studies, and described example implementation, presented in this white paper underscore the significant potential of the BCW to transform cybersecurity strategies across diverse industries. By meticulously analysing and addressing the specific components of behaviour - Capability, Opportunity, and Motivation - organisations can devise nuanced interventions that elevate their security practices beyond conventional measures. This approach not only enhances technical defences but also cultivates a robust and adaptive security culture, integral to withstanding the dynamic nature of cyber threats.

The adoption of the BCW framework enables organisations to systematically identify behavioural bottlenecks and strategically implement targeted changes that can lead to measurable improvements in cybersecurity outcomes. As demonstrated, interventions tailored to specific behavioural factors, such as enhancing motivation through incentives or increasing capability via education, can dramatically reduce vulnerabilities and foster a proactive stance on security.

Furthermore, the BCW provides a scalable model that can be adapted for various organisational sizes and types, from financial services to healthcare to e-commerce. This flexibility ensures that all organisations, regardless of their specific security challenges or cultural contexts, can benefit from a behaviourally informed cybersecurity strategy.

However, the journey towards a behaviourally mature cybersecurity culture is continuous and requires ongoing assessment and adaptation. Organisations should commit to regular evaluations of their cybersecurity behaviours and the effectiveness of implemented interventions. This dynamic approach ensures that as new threats emerge and technologies evolve, cybersecurity strategies remain effective and relevant.

In conclusion, integrating the Behaviour Change Wheel into cybersecurity strategies offers a comprehensive and effective method for enhancing not just the security infrastructure of an organisation but also the behavioural resilience of its workforce. By investing in behavioural change, organisations can anticipate better protection outcomes, reduced risk of breaches, and a security-conscious culture that inherently supports their overall mission and business objectives. This initiative-taking and behaviour-focused strategy signifies a mature approach to cybersecurity, positioning organisations to better navigate the complexities of the digital age.

References

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*, 6, 42.