CYBEHAVE

GUIDANCE

Title: Consolidated Framework for Implementation Research (CFIR) in Cybersecurity: A Practical Guide for Behavioural Change

Date: May 30th, 2025

Author: Andy Wood

Abstract:

The **Consolidated Framework for Implementation Research (CFIR)** provides a robust and structured approach for embedding cybersecurity behavioural change across complex organisations. Originally developed in healthcare, CFIR is now being successfully applied in cybersecurity to support the sustainable adoption of secure practices.

This guide introduces CFIR to security professionals with no prior background in behavioural science. It explains its five core domains—Intervention Characteristics, Outer Setting, Inner Setting, Characteristics of Individuals, and Process—and illustrates how they can be used to diagnose, plan, and evaluate behavioural change initiatives. A step-by-step walkthrough equips practitioners with practical tools to apply CFIR in real-world settings, while three real-life examples demonstrate its use in improving adoption of secure communication tools, scaling Security Champion networks, and increasing incident reporting.

By applying CFIR alongside models like COM-B and the Behaviour Change Wheel, security leaders can move beyond awareness campaigns and deliver long-lasting behavioural change grounded in evidence, context, and continual refinement.

Introduction

In the field of cybersecurity, technical solutions often overshadow the human factors that are just as critical to resilience. As the human element becomes more recognised, professionals are increasingly turning to behavioural science to drive meaningful change. One powerful but underutilised tool in this space is the Consolidated Framework for Implementation Research (CFIR). Although originally developed for healthcare, CFIR is highly applicable in cybersecurity, especially when implementing behavioural interventions across complex organisations.

This guide is designed to help cybersecurity practitioners understand, talk about, and apply CFIR with confidence, even without a background in behavioural science. It outlines the framework's background, relevance to cybersecurity, when to use it in the behavioural change process, how to apply it step-by-step, and provides three practical examples to ground the theory in reality.

CYBEHAVE

Background of CFIR

CFIR was developed in 2009 by Damschroder et al. to synthesise numerous implementation theories and models into a single coherent framework. It was originally designed to evaluate health service interventions but has since found utility in a wide range of disciplines where implementation in complex systems is required.

The framework includes five major domains:

1. **Intervention Characteristics** – the features of the intervention itself, such as complexity, adaptability, and perceived advantage.
2. **Outer Setting** – the broader environment outside the organisation, including stakeholder needs and external pressures.
3. **Inner Setting** – the internal environment within the organisation, including culture, communication, and resource availability.
4. **Characteristics of Individuals** – the traits, beliefs, and attitudes of the people involved in implementation.
5. **Process** – the actions and steps taken to plan, execute, and monitor the implementation effort.

Each domain includes specific constructs to help you evaluate and improve your behavioural change strategy comprehensively.

Why Use CFIR in Cybersecurity?

Cybersecurity interventions are rarely plug-and-play. Whether it's a new training module, a security policy, or a Champions network, these changes require uptake across diverse teams with differing priorities, pressures, and cultures.

CFIR is particularly powerful in cybersecurity because it:

- ✓ Helps you understand not just what needs to change, but **how and where** change is likely to be resisted or supported.
- ✓ Bridges the gap between **designing a behavioural intervention** and actually **embedding it in practice**.
- ✓ Encourages a system-wide view, recognising that even the best-designed behaviour change strategies can fail if organisational culture, leadership, or external pressures are not addressed.
- ✓ Provides a structured and evidence-informed approach to **tailoring interventions to context**, enhancing their relevance and impact.

CYBEHAVE

When to Use CFIR

CFIR is best used during the implementation planning and evaluation phases of behavioural change. It complements diagnostic models like COM-B and TDF, which help you understand behavioural barriers, and it builds on intervention design tools like the Behaviour Change Wheel. Think of CFIR as the bridge that takes your intervention from theory to real-world adoption.

You would use CFIR when:

- You are preparing to roll out a new security initiative that requires behaviour change.
- You need to tailor your intervention to different parts of the organisation.
- You want to understand why a previous initiative failed or struggled to gain traction.
- You are aiming to embed behavioural change long-term rather than one-off campaigns.
- You want to systematically evaluate the success and barriers of an ongoing behavioural programme.

Step-by-Step: Applying CFIR in Cybersecurity Behaviour Change

Step 1: Define the Intervention: Start by clearly defining the behavioural change you want to achieve. This might be improving phishing reporting, encouraging regular software updates, or embedding a 'secure by default' mindset in teams.

Be specific. What action do you want people to take, in what context, and why? This clarity will help guide the rest of the process.

Step 2: Use the Five CFIR Domains to Explore Implementation Factors: Approach each of the five domains with critical reflection and data gathering:

- **Intervention Characteristics** – Examine the perceived strength and complexity of your initiative. Is it easy to use? Does it offer clear advantages over current practices? Can it be adapted to local teams or roles?

- **Outer Setting** – Consider external influences, including customer expectations, regulations, and industry standards. Are there external motivators that could help, or pressures that may create friction?

- **Inner Setting** – Analyse internal structures. What's the general attitude towards cybersecurity in the organisation? Are communication pathways open? Are resources and leadership support in place?

- **Characteristics of Individuals** – Consider whether staff have the skills, knowledge, and confidence to adopt the change. What are their personal values, habits, and perceptions of cybersecurity?

- **Process** – Plan how the change will be introduced, supported, and refined. Who needs to be involved? What activities will raise awareness, build capability, and reinforce the change over time?

Step 3: Gather Data: Collect insights aligned to the five domains. Use a mix of qualitative and quantitative approaches such as:

- Staff surveys assessing confidence and perceived support
- Interviews with Champions and line managers
- Focus groups exploring cultural norms and communication gaps
- Observations of how current behaviours are enacted day-to-day

Step 4: Analyse and Interpret: Map the data to CFIR domains. Look for patterns. Are some teams facing resource challenges? Are others thriving because of strong leadership backing? This process turns raw insight into structured, actionable intelligence.

Step 5: Tailor Your Implementation Strategy: Now adapt your intervention. Use what you've learned to address barriers and enhance enablers. Examples include:

- Creating quick start guides for tools perceived as complex
- Running stakeholder briefings where leadership buy-in is weak
- Using peer-led sessions in teams with low self-efficacy

This tailored approach ensures that your initiative is context-sensitive and far more likely to succeed.

Step 6: Monitor and Iterate: Embed mechanisms to capture feedback regularly. This could be through ongoing surveys, informal check-ins with Champions, or analysis of behavioural data (e.g., click-through rates on awareness content).

Use these insights to refine your strategy. CFIR isn't static; it should inform a cycle of continuous learning and adaptation.

Real-World Examples of CFIR in Action

Example 1: Embedding a Secure Communication Tool

A large organisation introduced a secure messaging app to replace the informal sharing of sensitive documents via email. Although technically superior, uptake was low.

CFIR analysis revealed two issues. First, users perceived the new system as overly complex, and it didn't integrate well with daily workflows (Intervention Characteristics). Second, line managers hadn't promoted it, and some actively discouraged its use due to time pressures (Inner Setting).

The response included simplifying the interface, embedding the tool in everyday platforms like Microsoft Teams, and briefing managers on the benefits of compliance and productivity. Adoption rates grew within weeks.

Example 2: Launching a Security Champions Programme

A multinational rolled out a Security Champions network to embed cultural change. However, the programme stalled after an initial burst of enthusiasm.

A CFIR-informed review identified that external demands (Outer Setting), such as the need for rapid client delivery, left little time for Champions to engage meaningfully. Internally, many departments lacked structured support or clear expectations for the role (Inner Setting).

The intervention was revised to offer Champions bite-sized tools that saved time rather than added to workloads, and new line manager guidance helped reinforce the programme. This led to an expansion of the Champion network and more active participation.

Example 3: Improving Incident Reporting

An organisation noted under-reporting of cybersecurity incidents despite frequent awareness campaigns.

Using the CFIR, the team discovered that employees feared negative consequences for reporting (Characteristics of Individuals) and believed that incidents weren't being acted upon (Inner Setting).

To address this, a psychological safety policy was introduced, along with a transparent reporting process that highlighted outcomes and positive responses. Within six months, the rate of incident reporting had tripled.

Conclusion

The CFIR framework provides a comprehensive and structured approach to implementing behavioural change that lasts. For cybersecurity professionals, it brings a much-needed systems lens to what is often seen as an individual issue. By exploring not only what people should do, but also the entire ecosystem that supports or undermines their actions, CFIR helps practitioners transition from awareness to adoption to sustained cultural change.

When used alongside diagnostic models like COM-B and intervention design tools like the Behaviour Change Wheel, CFIR transforms your behavioural strategy from theory into practice. It helps you navigate complexity, build momentum, and ensure that secure behaviours take root and endure.