CYBEHAVE

GUIDANCE

Title:	Theoretical Domains Framework (TDF) in Cybersecurity: A Practical Guide for Behavioural Change
Date:	May 30th, 2025
Author:	Andy Wood

Abstract:

This guide introduces cybersecurity professionals to the Theoretical Domains Framework (TDF), a comprehensive behavioural science model designed to diagnose and address the underlying drivers of human behaviour. Originally developed for implementation research in healthcare, the TDF integrates 33 psychological theories into 14 practical domains, offering deep insight into why individuals may or may not adopt secure behaviours in the workplace. This resource provides clear guidance on when and how to use the TDF within the behavioural change process, particularly in diagnosing behavioural barriers, informing intervention design, and evaluating cultural impact. With step-by-step instructions and real-world cybersecurity examples, the guide enables practitioners with no prior background in behavioural science to confidently apply the TDF to everyday challenges, such as phishing under-reporting, weak engagement with Security Champions, and inconsistent adoption of security protocols. It positions the TDF as a vital tool for moving beyond awareness campaigns to deliver strategic, evidence-informed behavioural change that lasts.

Introduction

In cybersecurity, human behaviour is increasingly recognised as both a significant risk and a key defence mechanism. Yet changing behaviour across complex organisations is rarely straightforward. Traditional awareness programmes often fall short because they fail to address the real psychological, social, and environmental drivers of behaviour. This is where the **Theoretical Domains Framework (TDF)** becomes invaluable.

Originally developed for implementation research in healthcare, the TDF brings together constructs from 33 behavioural theories into a single, coherent framework. It provides a comprehensive lens for understanding the full range of factors that influence behaviour and is now widely used in applied behavioural science, including cybersecurity. It enables security professionals to design change initiatives with greater precision, ensuring the correct drivers are targeted rather than relying solely on awareness.

This guide is written for security professionals who may not have a background in behavioural science but are looking to understand and apply the TDF to diagnose behavioural problems, inform intervention design, and ultimately support cultural and behavioural change within their organisations.

Why Use TDF in Cybersecurity?

Cybersecurity behaviours, such as reporting phishing, locking devices, or updating software, depend on more than just knowledge. People may understand what to do, but that doesn't mean they will do it. TDF allows you to uncover deeper reasons for insecure behaviours, such as social expectations, emotional responses, identity conflict, or perceived lack of control.

TDF is beneficial in environments where multiple factors might be contributing to the same behavioural issue. For example, poor incident reporting may be due to fear of punishment (emotional factor), a perceived lack of importance (beliefs about consequences), or unclear reporting procedures (knowledge and environmental context). By identifying the dominant influences in your setting, you can design interventions that directly address them, thereby avoiding the scattergun approach of generic training or one-size-fits-all messaging.

TDF helps answer questions like:

- Why are staff still reusing passwords despite training?
- Why are incidents under-reported in specific departments?
- Why do some teams engage strongly with Security Champions while others don't?
- Why do certain employees continue to click on phishing links even after simulation campaigns?

By unpacking the psychological and contextual drivers behind these behaviours, TDF enables you to tailor your interventions to address the real root causes, not just the symptoms.

When to Use TDF in the Behavioural Change Journey

TDF is primarily used in the **diagnosis** and **understanding** phase of behavioural change. However, its insights can inform every stage of the process:

- **Diagnosing behaviour:** TDF helps you identify what's really influencing or blocking the behaviour, before you jump to solutions.
- **Understanding variation:** TDF helps explain why different departments or individuals may respond differently to the same awareness campaign or policy.
- **Designing interventions:** TDF identifies the most relevant domains to target, which can be matched with proven behaviour change techniques.

- **Supporting change agents:** Champions or influencers can be trained to recognise and address the TDF domains in everyday practice.
- **Evaluating change:** Repeat assessments of TDF domains can measure the underlying shift in beliefs, skills, or perceptions, not just behavioural outcomes.

TDF complements other frameworks, such as COM-B and the Behaviour Change Wheel (BCW). While COM-B provides a high-level diagnosis (capability, opportunity, motivation), TDF offers a detailed diagnostic lens underneath. Think of it as the 'deep dive' tool for complex or persistent behaviour challenges.

The 14 Domains of the TDF

Each of the TDF's domains represents a category of potential behavioural influence:

1. **Knowledge**: Awareness or understanding of cybersecurity risks, policies, or practices.
2. **Skills**: Practical or technical abilities, such as using a VPN or identifying suspicious URLs.
3. **Social/professional role and identity**: Whether people see secure behaviour as part of their role (e.g. "I'm not technical—it's IT's job").
4. **Beliefs about capabilities**: Confidence in their ability to perform the behaviour, sometimes linked to digital literacy.
5. **Optimism**: General belief that their actions will help and make a difference.
6. **Beliefs about consequences**: Perceptions of what will happen if they do or don't act securely.
7. **Reinforcement**: Past rewards or punishments that shape current behaviour (e.g. being blamed or praised).
8. **Intentions**: Whether people plan to perform the behaviour.
9. **Goals**: Competing demands that might deprioritise security (e.g. rushing to meet a deadline).
10. **Memory, attention and decision processes**: Forgetting, being distracted, or failing to notice cues for action.
11. **Environmental context and resources**: Time, tools, system design, workload, or physical settings.
12. **Social influences**: Peer pressure, leadership support, or cultural norms.
13. **Emotion**: Fear, anxiety, embarrassment, or stress influencing secure (or insecure) behaviour.
14. **Behavioural regulation**: Self-monitoring, reminders, prompts, and routines.

No single domain explains behaviour on its own. A combination of several domains shapes most behaviours, and the TDF helps map this landscape.

Step-by-Step Walkthrough of Using TDF

1. **Identify the target behaviour:** Clearly define the specific behaviour you are trying to influence. It must be observable and specific. For instance, rather than aiming to “improve cyber awareness”, define the goal as “staff consistently reporting phishing emails within two hours of receipt.”
2. **Collect data to diagnose the problem:** Use interviews, surveys, focus groups, or observational data. Structured interview guides based on the TDF domains can help reveal why the behaviour isn’t happening. Avoid assuming the problem is due to knowledge gaps—test each domain.
3. **Analyse and map findings to TDF domains:** Group your data by the 14 TDF domains. Look for recurring themes. For instance, a repeated mention of “not knowing how to identify phishing” aligns with the knowledge domain, while “I don’t think my manager would support me” aligns with social influences.
4. **Prioritise key barriers and enablers:** Some domains will appear more frequently or have a more substantial influence on the behaviour. These should be prioritised for intervention design. You may also consider domains that are easier to influence or more feasible to address in the short term.
5. **Select behaviour change techniques:** Use the Behaviour Change Wheel to match domains with relevant intervention functions (e.g., training, modelling, enablement) and behaviour change techniques (e.g., action planning, feedback, rewards).
6. **Design your intervention:** Translate these techniques into practical, context-sensitive activities or strategies. If a lack of confidence (in beliefs about capabilities) is the issue, you might consider developing a peer mentoring programme. If emotion is the barrier, you might address fear through storytelling and reassurance.
7. **Implement and evaluate:** Roll out the intervention and evaluate its effect on the behavioural domains, not just the behaviour itself. For example, does confidence increase? Do employees feel reporting is easier or more supported? This gives you data for iterative improvement.

Real-Life Examples in Cybersecurity

Below are three real-life use-case examples to help bring this guide to life.

Real-Life Example 1: Under-Reporting of Phishing Emails

A company experienced low rates of phishing email reporting, despite having trained its staff. Interviews revealed that staff were hesitant to report because they feared looking foolish (emotion), weren't sure what qualified as a phishing email (knowledge), and didn't see their peers doing it (social influences).

Using this insight, the company:

- Created a clear visual guide to identifying phishing (addressing knowledge).
- Ran a campaign where leaders praised individuals who reported emails (reinforcement).
- Shared team-wide stats to normalise reporting (social influence).

Reporting rates increased by 40% over a three-month period.

Real-Life Example 2: Weak Engagement with Security Champions

A security team rolled out a Champions programme, but some departments were disengaged. TDF-guided interviews highlighted two main issues: many didn't see security as their responsibility (social/professional role), and some Champions lacked confidence (beliefs about capabilities).

Interventions included:

- Incorporating security tasks into formal job descriptions (role identity).
- Running peer-led training sessions to boost Champion confidence (skills and beliefs about capabilities).

This led to improved Champion engagement and peer influence within those departments.

Real-Life Example 3: Inconsistent Use of Two-Factor Authentication (2FA)

A multi-site organisation found that staff in some offices adopted two-factor authentication (2FA), while others resisted. TDF analysis revealed that in offices where 2FA was resisted, people believed it would slow them down (beliefs about consequences), were unsure how to set it up (skills), and hadn't seen their team leaders using it (modelling).

To address this:

- Quick-start guides were issued to simplify setup.
- Local leaders demonstrated 2FA use during meetings.
- Teams were given feedback on how their adoption compared to others.

Adoption in resistant sites rose by over 60% in two months.

Conclusion

The Theoretical Domains Framework gives security professionals a rich, structured approach to understanding the true drivers of behaviour. It helps you move beyond assumptions and surface-level solutions to create tailored, psychologically grounded interventions that actually work.

By embedding the TDF into your behavioural change approach, you can become more strategic, evidence-based, and ultimately more effective in your role. Whether you're trying to improve incident reporting, boost secure habits, or scale culture change, TDF enables you to understand people more deeply and change behaviour more effectively. With the step-by-step approach and examples in this guide, you now have a practical starting point to apply TDF in your cybersecurity initiatives confidently.

Engage. Educate. Empower.

https://CyBehave.org