CYBEHAVE

GUIDANCE

Title: Self-Determination Theory (SDT) in Cybersecurity: A Practical Guide for Behavioural Change

Date: May 30th, 2025

Author: Andy Wood

Abstract:

This guide provides cybersecurity professionals with a comprehensive, practical introduction to **Self-Determination Theory (SDT)** as a framework for influencing secure behaviour. Rooted in psychological science, SDT focuses on intrinsic motivation by satisfying three core human needs: autonomy, competence, and relatedness. The guide explains the background and relevance of SDT within the broader context of behaviour change, and outlines how it complements established models such as COM-B and TDF. It includes a step-by-step application process, enabling professionals to design and embed long-term behavioural interventions that move beyond compliance. Three real-world case studies illustrate the theory in action, ranging from Security Champions networks to phishing reporting and onboarding. This resource equips security leaders with the confidence and tools to apply SDT effectively, fostering a culture where secure behaviour is both meaningful and sustainable.

Introduction

Self-Determination Theory (SDT) is a well-established theory of motivation in psychology, developed by Edward Deci and Richard Ryan in the 1980s. Unlike many behaviour change theories that focus on external drivers (such as punishment or reward), SDT explores the intrinsic motivation behind human behaviour. It helps us understand how to create environments where people choose to behave in specific ways because they want to, rather than being forced to.

This guide is designed to help security professionals understand and apply SDT to drive behavioural change in their organisations, particularly where culture, engagement, and human resilience to cyber threats are the focus. Whether you are launching a secure behaviour campaign, building a Security Champions network, or trying to embed everyday secure practices into workplace culture, SDT can be a powerful tool in your behavioural change arsenal.

CYBEHAVE

Background of SDT

At its core, SDT proposes that individuals are more likely to adopt and maintain behaviours when three psychological needs are met:

- **Autonomy**: The need to feel that one's behaviour is self-endorsed and aligned with personal values. People are more likely to act securely if they feel the choice is theirs and it aligns with their own beliefs about what is right.
- **Competence**: The need to feel effective, capable, and confident in one's actions. If someone believes they can spot a phishing email or create a strong password, they are more likely to do so.
- **Relatedness**: The need to feel connected to others, part of a group or community. Secure behaviours are more likely to be adopted when people feel their actions contribute to team success or protect others.

In cybersecurity, SDT helps us move beyond short-term compliance driven by fear or rules, towards internalised, meaningful engagement with secure behaviours.

Why Use SDT in Cybersecurity?

Many traditional security interventions rely on external motivators, such as mandatory training, sanctions for non-compliance, or rigid policies. While these tools can establish a baseline of security, they rarely lead to lasting change. They can even generate resentment, disengagement, or behaviour that is performed only when under supervision.

SDT offers an alternative: a way to foster motivation that lasts beyond enforcement. It allows us to build a security culture where behaviours are internalised and become part of everyday routines because they make sense to people personally and socially. It helps to:

- ✓ **Encourage genuine buy-in** to security messages and protocols
- ✓ **Strengthen the emotional connection** to security (e.g., protecting colleagues and customers)
- ✓ **Promote proactive behaviour**, such as voluntary reporting or seeking help
- ✓ **Increase trust** between the security function and wider teams

This approach is instrumental in building resilience in distributed workforces, influencing line managers, and embedding behaviours in hybrid or high-autonomy teams.

Where SDT Fits in the Behavioural Change Process

In the bigger picture of behaviour change, SDT plays a crucial role across multiple stages:

- **Understanding motivation**: Use SDT to determine why people act as they do. Are they motivated by obligation, habit, fear, or personal values? This insight can influence the direction of interventions.
- **Designing interventions**: Once motivational drivers are clear, interventions can be designed to satisfy the three SDT needs. This makes behaviour change more natural and less resistant.
- **Sustaining behaviour**: SDT is particularly effective for embedding and sustaining secure behaviours over time. People are more likely to continue secure practices if they feel competent, supported, and in control.

While SDT isn't a diagnostic tool like COM-B or TDF, it complements them by giving depth to the motivational aspects of behaviour and providing a human-centred lens through which to design change strategies.

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

1. **Understand your audience's current motivation:** Begin by exploring the reasons why people engage in (or avoid) particular behaviours. For example, do staff complete mandatory security training because they are genuinely interested, or simply to comply with a requirement? Use surveys, focus groups, or casual conversations to uncover motivational factors. Pay attention to language: words like "have to" and "required" suggest external motivation; words like "useful" or "important to me" suggest internal motivation.
2. **Identify gaps in autonomy, competence, or relatedness:** Map the barriers and enablers in your current culture. If people feel overwhelmed by complex policies, there may be a competence gap. If they feel forced into processes without explanation, it's an issue of autonomy. If they view the security team as outsiders or enforcers, relatedness is missing. These gaps tell you where to focus your intervention design.
3. **Design interventions to foster autonomy:** Autonomy doesn't mean removing all rules—it means helping people understand and connect with the reasons behind them. Provide rationale for security policies and make training feel relevant. Allow for choice where possible, such as different learning formats or channels for reporting incidents. Invite feedback and involve employees in shaping interventions. This increases ownership and reduces resistance.
4. **Support competence:** Build people's belief in their ability to act securely. Avoid jargon and complexity. Offer real-life scenarios, simple instructions, and hands-on opportunities to practice. Celebrate success stories and recognise progress. If someone

flags a suspicious email, thank them and highlight the positive impact of their action. These moments build confidence and reinforce a sense of skill.

5. **Build relatedness:** Show that cybersecurity is not just a technical issue but a social responsibility. Use storytelling to demonstrate how secure behaviours protect real people. Encourage teams to share tips and lessons learned. Create peer-led communities, such as Champion networks or buddy systems, to foster collaboration. When people feel they're part of a team effort, secure behaviours are more likely to stick.
6. **Reinforce without coercion:** Replace blame-based approaches with constructive reinforcement. Offer guidance when mistakes happen. Use behavioural nudges like prompts, checklists, or friendly reminders to keep behaviours front of mind. Reinforce the value of secure behaviours with recognition, not reprimand. Over time, this builds a psychologically safe environment where people feel able to try, fail, and learn.
7. **Evaluate and iterate:** Behaviour change is an ongoing process. Use qualitative feedback, behaviour tracking, and conversations to assess how people feel about the interventions. Are they becoming more confident? Do they understand why security matters? Are secure behaviours becoming routine? Adapt your strategy based on what works and where the three SDT needs are still unmet.

Real-World Examples of CFIR in Action

Example 1: Security Champions Programme

A large UK-based organisation was struggling with an inactive Champions network. Participation was low, and most Champions had been nominated without consent. By redesigning the programme around SDT, they introduced a voluntary sign-up system, allowing people to choose the level of involvement that suited them, thereby satisfying autonomy. They provided structured training paths with options to specialise, supporting competence. They created a monthly community of practice and peer coaching, building relatedness. Within six months, Champion engagement increased by 40%, and reports of positive peer influence on security behaviours tripled.

Example 2: Phishing Reporting Campaign

A company's phishing simulation programme was causing stress and disengagement. Employees feared 'failing' the test. The security team reframed the campaign using SDT. Instead of punishing clicks, they celebrated reporting. Real stories were shared, highlighting how a reported email protected a team. Staff received thank-you messages and small team-level rewards for engagement. Reporting rates increased steadily, and staff interviews showed greater confidence and motivation to stay alert, not because they had to, but because they wanted to help their colleagues.

Example 3: Onboarding Secure Behaviour

A major retail brand revised its onboarding process to make secure behaviour part of the employee journey from day one. New starters were offered a choice of learning formats, ranging from short explainer videos to interactive walkthroughs, which supported autonomy. The content was tied directly to customer protection and operational success, reinforcing their relatedness. Small, immediate actions—like setting up secure passwords and learning how to spot suspicious activity—were linked to practical tasks, building competence. Security behaviours were reported as 'normal' and 'expected' by new hires within their first month.

Conclusion

Self-Determination Theory is a powerful yet often overlooked framework in cybersecurity behaviour change. By tapping into the core psychological needs of autonomy, competence, and relatedness, SDT allows us to move beyond tick-box compliance and into genuine, sustained behavioural engagement. When people choose to act securely because it aligns with who they are, how they want to feel, and the teams they care about, change becomes embedded and enduring.

Whether you are designing a new awareness initiative, relaunching your Champions network, or embedding cyber-safe habits across the workforce, SDT offers a grounded, human-centred approach that empowers people to make the secure choice because they want to. With this guide, you now have the knowledge, process, and real-world examples to confidently apply SDT in your cybersecurity practice and drive meaningful, lasting change.