CYBEHAVE

GUIDANCE

Title: Diffusion of Innovations in Cybersecurity: A Practical Guide for Behavioural Change

Date: May 30th, 2025

Author: Andy Wood

Abstract:

This guide introduces cybersecurity professionals to the **Diffusion of Innovations (DoI)** theory, a robust framework for driving and sustaining secure behaviour change across organisations. Grounded in sociological research, DoI explains how new behaviours, practices, or technologies are adopted over time by different segments of a population. The guide explores how DoI complements other behavioural models such as COM-B, the Behaviour Change Wheel, and Social Network Analysis, and positions it within the "understanding" and "design" phases of cybersecurity behaviour change strategies. Through a straightforward step-by-step application process and real-world examples—including phishing reporting, secure file-sharing adoption, and cultural shifts in incident reporting—this guide equips professionals with the practical knowledge needed to identify early adopters, scale influence, and institutionalise long-term change. It is designed for those without prior behavioural science training, making DoI accessible, actionable, and relevant to modern cybersecurity leadership.

Introduction

In today's digital-first world, security professionals are expected not only to manage threats and technical controls but to drive behavioural change across their organisations. To do this effectively, we must understand how new ideas, behaviours and practices spread through a population. This is where the Diffusion of Innovations (DoI) theory becomes invaluable.

Originally developed by Everett Rogers in the 1960s, DoI is a sociological model that explains how innovations, which can include new technologies, behaviours or practices, are adopted over time within a social system. For cybersecurity, this could mean adopting multi-factor authentication, reporting phishing attempts, or fostering a culture of incident reporting.

This guide is designed to help security professionals with no prior training in behavioural science understand and apply DoI to support lasting cybersecurity change. With the right approach, you can convert early momentum into a lasting cultural transformation.

CYBEHAVE

Why Use Diffusion of Innovation in Cybersecurity?

Cybersecurity isn't just about the controls you deploy; it's about how people adopt and sustain secure behaviours. Often, safe practices are seen as an "innovation" within teams, particularly if they disrupt routines, require effort to learn, or challenge existing habits. Resistance to change is not always about rejection—it's often about the timing and perceived effort involved.

DoI gives us a structured lens through which to understand this change journey. It enables security professionals to plan the strategic introduction and scaling of new practices. Rather than pushing everyone to adopt a behaviour simultaneously, DoI shows how to create influence through social modelling and phased adoption.

It is instrumental when launching:

- ✓ New security tools or platforms
- ✓ Organisational culture change programmes
- ✓ Cybersecurity policies or behavioural norms (e.g. secure sharing, password hygiene)
- ✓ Incident response or breach reporting protocols

By recognising how behaviours spread and who influences that spread, security teams can make smarter decisions about communication, training, timing, and reinforcement.

Where Diffusion of Innovations Fits in Behavioural Change

In the broader field of behavioural change, models like COM-B help us understand what needs to change, such as gaps in capability, motivation, or opportunity. The Behaviour Change Wheel (BCW) helps define the types of interventions that will support the change, such as education or enablement. Social Network Analysis (SNA) shows who is influential and how information travels.

The Diffusion of Innovations complements these tools by examining *how change spreads across a population over time*. It provides insight into the psychology of adoption, group dynamics, and the social tipping points that make behaviours stick.

In particular, DoI is useful in the "understanding" and "designing" phases of behaviour change planning. It helps you identify entry points, choose target audiences, and scale impact based on peer influence, rather than relying solely on coercion or policy enforcement.

The Five Adopter Categories

Rogers identified five distinct types of adopters within any population:

- **Innovators** are the risk-takers and experimenters. They often have deep domain knowledge, curiosity, or a natural inclination to explore. In cybersecurity, these may be technical teams or early testers of new platforms. They are often unconcerned with norms and more interested in novelty and problem-solving.
- **Early Adopters** are respected individuals whom others turn to for guidance. They are open to new ideas but selective and strategic. In a security context, these may be well-regarded line managers, Security Champions, or those with strong interpersonal influence. Their visible adoption can provide essential validation for the rest of the workforce.
- **Early Majority** are more cautious but pragmatic. They wait for proof of success and want to see others benefiting before they adopt. They are essential to reaching a critical mass but require reassurance, training, and support.
- **Late Majority** are risk-averse and conservative. They adopt out of necessity, often due to pressure from colleagues or policy mandates. They respond better to structured processes, strict enforcement, and broad evidence that "everyone else is doing it."
- **Laggards** are the last to adopt. They often hold strong attachments to past behaviours or distrust the change itself. While they should not be ignored, focusing on them too early can waste effort. Strategies for laggards should rely on policy, consistency, and ongoing reinforcement rather than persuasion.

Understanding which groups your staff fall into allows you to shape the right messaging, support, and timing for each segment.

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

Step 1: Define the Innovation Clearly: Before any change effort begins, be specific about what the "innovation" is. Is it a tool, a behaviour, a cultural practice? What precisely do you want people to do differently? Frame it in a way that highlights its relevance, simplicity, and benefit.

For example: "We want employees to use our secure document-sharing platform instead of emailing sensitive files."

Step 2: Assess the Innovation's Perceived Attributes: Five key attributes influence how fast an innovation spreads:

1. Relative Advantage: Is this better than the current behaviour?
2. Compatibility: Does it align with existing values and practices?
3. Complexity: Is it easy to understand and use?
4. Trialability: Can people try it without full commitment?
5. Observability: Will others see them benefiting from it?

By shaping how the innovation is presented, you increase its appeal. Highlight success stories. Offer demos. Make it visible.

Step 3: Segment and Understand Your Audience: Use simple staff interviews, digital feedback, or SNA to determine who your innovators and early adopters are. These people are your leverage points. They will set the tone for adoption by the wider group.

Step 4: Tailor the Rollout to Each Group: Don't aim for a single "big bang" rollout. Start small and build influence. Pilot the change with innovators and early adopters. Collect data, success stories, and testimonials. Share these internally.

Once the early adopters have visibly embraced the behaviour, move to engage the early majority. Provide extra resources, training, and social proof. Save structured compliance-driven approaches for the late majority and laggards, who require certainty and strong policies.

Step 5: Build Feedback and Monitor Progress: Track uptake through system analytics, behavioural observations, and surveys. Look for indicators like frequency of secure file sharing, reduction in USB use, or phishing reports. Share progress and success stories widely.

Step 6: Sustain and Institutionalise the Change: As adoption increases, embed the behaviour into policy, onboarding, regular training, and leadership expectations. Make the secure behaviour the default. Continue to reward and celebrate those who model the change.

Real-World Examples of DoI in Action

Example 1: Encouraging Phishing Email Reporting

A financial services firm sought to increase staff awareness of phishing attempts. Instead of a generic company-wide campaign, they began with cyber-savvy teams, such as IT and risk management. These innovators were coached on what to look for and how to report. Early success stories were shared through the company's internal news feed. Security Champions (early adopters) then modelled the behaviour in town halls. Within two months, phishing reports increased by 45%, and the majority of staff viewed it as a "normal" responsibility.

Example 2: Replacing USB Drives with Secure File Transfer Tools

A manufacturing company needed to eliminate USB use due to regulatory risk. Rather than issuing an immediate ban, they piloted a secure collaboration platform with a small group of project managers known for their openness to digital tools. The feedback from this group was used to develop user guides and training materials. The innovation was then expanded to teams in engineering and procurement. Only once the uptake had passed 75% were USB ports disabled.

Example 3: Creating a Culture of Security Incident Reporting

In a university, staff members were reluctant to report incidents for fear of being blamed. A new non-punitive incident reporting system was introduced. Innovators within the IT and cybersecurity teams led by example, submitting minor incidents and explaining the learning outcomes in newsletters. Department heads (early adopters) followed suit. As a result, other teams began submitting reports. Within a year, incident reporting doubled, and the quality of incident data significantly improved.

Conclusion

Diffusion of Innovations is not just a theory; it's a strategic tool that provides security professionals with a structured approach to spreading secure behaviours. It shifts the focus from enforcement to enablement, from blanket policies to social influence.

By using DoI you can build a roadmap that recognises human diversity in adoption readiness and leverages natural social dynamics to embed security at scale. Whether you're introducing a new reporting policy, retiring outdated tools, or encouraging cultural shifts, this model provides clarity on how to launch, sequence, and sustain effective behaviour change.

When combined with tools like COM-B, BCW, and SNA, the Diffusion of Innovations provides a comprehensive behavioural change toolkit, grounded in science, guided by human insight, and focused on results.