Driving Behavioural Change in Cybersecurity Course

Who should attend?

No prior technical cyber knowledge is required for this course, which focuses on leadership, decision-making, and behavioural risk management. This is designed for senior leaders, managers, and decision-makers responsible for people, process, and risk within an organisation; it is particularly relevant for:

- **Department heads and team leaders**
- **Programme and project managers**
- **Risk, compliance, and governance professionals**
- **Security leaders and non-technical executives**

Key Organisations

Ministry of Defence

Government Departments and Agencies

Defence and Security Organisations

Critical National Infrastructure (CNI) Providers

Large Commercial Enterprises and SMEs

Any organisation seeking to improve cyber resilience through leadership and culture

Introduction

Organisations invest heavily in cybersecurity technology and breaches still occur. Why? Because security failures are rarely caused by a lack of tools, but by a lack of alignment between people, process, and behaviour.

This course is designed to equip management with the knowledge and practical tools required to drive meaningful behavioural change in cybersecurity. It challenges traditional approaches that rely solely on policy enforcement and technical controls, and instead focuses on how leadership decisions shape organisational behaviour both positively and negatively.

Through a combination of real-world case studies, behavioural models, and scenario-based exercises, participants will learn how to identify hidden risks, reduce friction, and create an environment where secure behaviour becomes the default, not the exception.

A key feature of this course is its practical application. Throughout the day, participants will work collaboratively to develop a tailored cyber security action plan, aligned to their organisational context. By the end of the course, attendees will leave with a structured model and clear, actionable steps that can be immediately implemented to initiate meaningful change within their organisation.

What you will learn:

- Why traditional cybersecurity approaches (People, Process, Technology) often fail in practice
- How behavioural biases influence decision-making and create hidden vulnerabilities
- The impact of organisational culture on cyber security outcomes
- How to identify and reduce “shadow security practices” within teams
- How to interpret technical risk (e.g. CVSS reporting) in a business context
- The role of management in bridging the gap between security teams and operations
- How to design and implement effective behavioural change strategies
- Practical frameworks for improving adoption of security controls (e.g. ADKAR, behavioural models)
- How to communicate cyber risk in a way that drives action and accountability
- Techniques for building a security-conscious culture without creating friction or resistance

Course Duration
1 Day

Location
Mercury EW Ltd – Training Facility or Customer Site