CYBEHAVE · INTERMEDIATE

Behavioural Risk in Practice

Course workbook

Design, deliver and measure interventions that shift secure behaviour.

Build Behaviour. Build Culture. Build Resilience.

This workbook belongs to

Organisation and role

The one behaviour I am working on

cybehave.com/training · © 2026 CyBehave. All rights reserved. For use alongside the Behavioural Risk in Practice video course.

BEFORE YOU START

How to use this workbook

Foundations gave you the science. This course is about using it on a real team, under real pressure, and this workbook is where that happens. It follows the nine videos in order. Each module section gives you the key ideas in one place, the templates the video refers to, a short worked example from Marcus, and the five Reflect & Apply questions with room to write.

Five ways to get the most from it

1. **Move at your own pace.** The modules build on each other, but there is no clock. Pause whenever an idea needs to land.
2. **Bring one real behaviour.** Choose a behaviour in your own organisation you would genuinely like to change, and run every tool in this course against it. Each section has a "Your one behaviour" box for it. By module 5 you will have a one-page strategy.
3. **Use the templates, do not read them.** The observation grid wants an hour in a real meeting. The interview guide wants a coffee with a real colleague. Blank templates teach nothing.
4. **Apply as you go.** Observe someone this week. Rewrite one message. Try one conversation you have been putting off.
5. **Bring a human lens.** Curiosity over judgement. We are not just securing data; we are changing how people think, feel and act.

The course at a glance

Module	Title	Tools in this workbook
0	Welcome	Your one behaviour; meet Marcus.
1	Behavioural Influence in Complex Environments	Context map; influence inventory.
2	Advanced Diagnosis with COM-B	Behavioural Observation Grid; Human Risk Interview Guide; Behavioural Diagnosis Map.
3	Building Multi-Layered Interventions	Nine-function reference; layering canvas; what I left out and why.
4	Messaging, Framing and Cyber Nudges	Framing worksheet; nudge designer and ethics test; tone rewrites; Cyber Message Pack (30 examples).
5	Strategy Design for Human Risk	Behavioural objective builder; business alignment; culture readiness check; one-page strategy; rhythm planner.
6	Embedding Change and Measuring Behaviour	Habit loop; embedding in rituals; behavioural KPI set; feedback-loop planner.
7	Leading Human-Centred Security	Influence map; story bank; Champions network starter; 30/60/90 leadership plan.
8	Close	Seven ideas; one thing on Monday; glossary; further reading.

Three lines you will hear again

Start with the context, not the tool. · Diagnose before you design. · Lead from where you are.

WORKED EXAMPLE

Meet Marcus

Foundations followed Sally, the person whose behaviour needed to change. This course follows the person doing the changing. Marcus is the security culture lead at a logistics firm of about 1,200 people. He is good at his job, he cares about it, and he has no line authority over anyone he needs to influence.

The situation	Where the course takes it
The finance team (about forty people) report suspicious emails slowly: median nine hours, often never.	Module 1: the context map shows friction, a blame signal and a norm set by the manager.
Finance approves supplier payments, so invoice fraud is the live risk. One near-miss this year was worth £180,000.	Module 2: observation and interviews show capability is strong; opportunity is the dominant barrier.
Two awareness campaigns have already run. "We did that."	Module 3: a five-layer stack, with no third campaign in it.
The finance manager believes reporting is IT's job.	Module 4: messages in the team's own language: protect the payment run.
Odd emails already go to Dee, "who knows about this stuff".	Modules 5 to 7: a one-page strategy, ninety-day results, and Dee becomes the first Champion.

Use Marcus as a mirror

Each time a Marcus card appears, ask: what is the equivalent for my one behaviour? Who is my Dee? What is my "we did that"? Which manager sets the norm, and what would it take for them to co-sign the plan?

MODULE 1

Behavioural Influence in Complex Environments

Key ideas from the video

- Real life does not care about your framework. Behaviour change is less like flipping a switch and more like tuning an instrument: adjust, listen, retune.
- People follow what feels safe, accepted and possible, not always what is correct. Social norms, fear of blame, friction and the metrics people are measured on hold behaviour where it is.
- When the context is broken, the person is not. Surface the invisible forces before you choose a tool.
- Context mapping: study the system the person operates in, not the person. Pressures, friction points, what leaders and peers model, shadow systems.
- Influence without authority comes from credibility, consistency and empathy. Change happens through moments, not mandates.

Template: the context map

Pick one behaviour and one team. Spend an hour where the behaviour happens (a meeting, a process, a system) and fill the four quadrants from what you see and hear, not from what you assume.

Visible pressures	Friction points in process or tools

What leaders and peers model (even unintentionally)	Shadow systems and workarounds that have become normal

Marcus's map, in one line each

Pressures: quarter-end payment runs, a team working through lunch.

Friction: invoices arrive as forwarded PDFs inside the payments system; the report button lives in Outlook.

Modelled: the manager treats reporting as IT's job; nobody in finance has reported in three months; the last reporter got a "false alarm" reply.

Shadow system: odd emails go to Dee. An asset, not a workaround to stamp out.

Template: influence inventory

Where do people already listen to me?	Where do I see friction I could name?	Where could I create space for someone to speak up or slow down?

Your one behaviour

Write your one behaviour as a first draft: who does (or does not do) what, roughly how often, and what it costs. You will sharpen it into a behavioural objective in module 5.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. **Where have you seen behaviour driven by pressure, not policy?**

2. **What invisible forces might be shaping behaviour in your context?**

3. **How could you start observing behaviour in its environment, not in isolation?**

4. **What is one way you could influence secure behaviour without formal authority?**

5. **What will you commit to modelling differently, starting today?**

MODULE 2

Advanced Diagnosis with COM-B

Key ideas from the video

- COM-B is a lens for asking better questions, not a model to memorise. Move from "what happened?" to "why was that the best option at the time?"
- Indicators: capability shows as hesitation, errors and reliance on others; opportunity as friction, time pressure and conflicting systems; motivation as apathy, cynicism and fear. The absence of behaviour is just as telling.
- Three tools: the Behavioural Observation Grid (behaviour as data), diagnostic interviews (the why, if people feel safe), and the Behavioural Diagnosis Map (where to focus).
- Five examples of the same friction point and you are no longer guessing. You are building a case.

Template: Behavioural Observation Grid

Use it in a real setting: a process walkthrough, a team meeting, a system session, an incident review. Record what you see, not what you conclude. Roles, never names for blame.

What happened	Where and when	Who (role)	Said, or not said	C / O / M	Confidence

Look for consistency (the same behaviour across teams), repeated workarounds, and moments where even confident people hesitate.

Template: Human Risk Interview Guide

Not an audit. A conversation built on curiosity, empathy and safety. Twenty minutes, one person, one behaviour. Let them talk, reflect back what you hear, and thank them.

Opening questions

- "Tell me what happens when you receive a suspicious email."
- "What is the easiest part of following the guidance? What is the hardest?"
- "Can you recall a time something felt risky, and what you did?"
- "If you could change one thing about how security works here, what would it be?"

Follow the thread

If they talk about...	You are hearing...	Follow-up prompt
Confusion, not knowing the steps, "I'd ask someone"	Capability	"What would make you feel confident doing it yourself?"
Time pressure, clunky tools, "the system won't let me"	Opportunity	"Walk me through the steps as they actually happen."
Fear, frustration, "no one else does", "not my job"	Motivation	"What happened the last time someone did it?"
Hesitation, deflection, a change of subject	Something unsaid	Pause. "Tell me more about that."

Notes

What they feel capable of	What their environment enables or blocks	How they think and feel about it

Template: Behavioural Diagnosis Map

One target behaviour in the centre: specific, observable, security-relevant. Under each branch, the barriers and the enablers you found. Mark the dominant barrier; that is where you act first.

Target behaviour (who does what, by when)

Capability: barriers / enablers	Opportunity: barriers / enablers	Motivation: barriers / enablers

Dominant barrier	What is already working that we can build on

Marcus's completed map

Target: finance reports suspicious invoices within one hour (median today nine hours).

Capability: strong. The team spot odd invoices quickly. Small gap: what counts as reportable.

Opportunity: dominant barrier. Wrong window, too many steps, no time at quarter-end.

Motivation: fear of the "false alarm" reply; a norm that reporting is IT's job.

Enabler: Dee, and a team that already talks to each other about odd invoices.

Your one behaviour

Run the grid for one hour and have two interviews. Then fill the map for your one behaviour. Which branch is dominant?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. **What behaviour in your organisation needs better diagnosis?**

2. **Which COM-B element feels like the main barrier, and why?**

3. **Have you seen signs of low capability, poor opportunity or weak motivation?**

4. **Who could you observe or interview to gather real insight?**

5. **How could a Behavioural Diagnosis Map guide your next intervention?**

MODULE 3

Building Multi-Layered Interventions

Key ideas from the video

- Nine functions, one rule: match the function to the barrier. Do not default to what is familiar.
- Education, training and enablement are essential when capability is the gap and noise when it is not.
- Persuasion and modelling change how people feel and what they see: this is important, this is normal, this is something I can do.
- Nudges, environmental restructuring and friction design reshape the decision moment so it stops relying on memory or willpower.
- Restriction and coercion only when risk is high, the behaviour persists and other options have been tried, and always paired with support.
- Layer two or three functions that reinforce each other. More is not better; clarity beats complexity.

Reference: the nine intervention functions

Function	What it does	Use when the barrier is...	Cyber example
Education	Increases knowledge or understanding	Psychological capability (knowing)	Three real invoices in a ten-minute huddle
Training	Builds a specific skill	Physical or psychological capability (doing)	Hands-on secure file transfer
Enablement	Removes barriers, adds means	Capability or physical opportunity	Password manager; one-click report
Persuasion	Emotion or argument to motivate	Reflective motivation	"Protect your team. Speak up early."
Modelling	Shows the behaviour to imitate	Social opportunity, automatic motivation	The manager reports one in the team meeting
Incentivisation	Expectation of reward	Reflective motivation	Recognition in the team channel
Coercion	Expectation of cost or punishment	Reflective motivation (last resort)	Enforced policy in a regulated process
Environmental restructuring	Changes the physical or social context	Opportunity	Report button where the work happens; a thank-you reply
Restriction	Rules that limit the opportunity	Opportunity (high-risk paths)	Call-back before any bank-detail change

Template: the layering canvas

Start from the diagnosis map. One row per barrier. Each layer answers one barrier; if a row has no barrier, it is activity, not intervention.

Barrier (from the map)	Function	Specific action	Owner	Ethics check (transparent, fair, proportionate?)

Template: what I left out, and why

The discipline of layering is as much about what you do not add. Name the obvious interventions you are choosing not to run, and the diagnosis that rules them out.

Not doing	Because the map says

Marcus's stack

Enablement: one-click Report inside the payments system, forwarding to the security mailbox.

Environmental restructuring: the "false alarm" auto-reply becomes a thank-you that says what was checked.

Restriction (surgical): any supplier bank-detail change needs a call-back on a known number.

Modelling: Dee becomes the visible go-to; the manager reports one herself in the Monday meeting.

Education, small: a ten-minute huddle on what counts, with three real invoices.

Left out: a third awareness campaign (capability was never the barrier), coercion (a blame signal was already part of the problem), an incentive scheme (reporting should feel normal, not paid for).

Your one behaviour

Build the stack for your one behaviour: two or three layers, each pointing at a branch of your map.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. **Which intervention function have you used most often, and why?**

2. **Where might layering improve the results of your current approach?**

3. **Can you match a function to a real COM-B barrier in your environment?**

4. **What is one behaviour you would like to influence with a smarter mix of interventions?**

5. **How will you make sure your interventions are ethical, proportionate and human-centred?**

MODULE 4

Messaging, Framing and Cyber Nudges

Key ideas from the video

- Same information, different frame, different behaviour. Gain and loss frames both have a place; social proof works when it is true; one message per moment.
- Cyber nudges work at the moment of decision: timely, seven to ten words, neutral or positive tone, visually supported.
- The ethics test: transparent? easy to decline? in their interest? Three yeses and it is a nudge. Any no and you are designing something else.
- Tone, timing and language: second person, action verbs, short sentences, before the behaviour rather than after the mistake.
- A Cyber Message Pack: start with the diagnosis, choose the tone, keep it under twelve words, time it to the moment, make the behaviour feel normal, safe and valuable.

Template: framing worksheet

The message as it is today	Gain frame	Loss frame	Social proof version (only if true)

Template: nudge designer

The moment (what the person is about to do)	The nudge (7 to 10 words)	Channel and visual	Tone check

The moment (what the person is about to do)	The nudge (7 to 10 words)	Channel and visual	Tone check

Ethics test	Yes / No	If no, what changes?
Transparent: would people be comfortable if they knew exactly how and why it works?		
Easy to decline: can someone take the other path without penalty or embarrassment?		
In their interest: does it serve the person and their team, not just the metric?		

Template: tone rewrites

Sounds like a lecture	Sounds like help
"You must not store files here."	"Here's a secure place to keep your files."
"Users are reminded that policy requires..."	"Take ten seconds to protect your team."
"WARNING: You are sending an email externally."	"Heads up: this address is outside your organisation."

The Cyber Message Pack: thirty examples to adapt

Grouped by the moment they serve. Edit the words to your systems and your people; keep them under twelve words.

Before sending or sharing (opportunity, friction)

- Pause: external address detected. Check before sending.
- Heads up: this address is outside your organisation.
- Sharing outside the company? Use the secure link, not the file.
- New bank details? Confirm by phone first.
- Personal email? Keep work files on work systems.
- This folder is public. Sure that's what you want?

Before clicking or opening (capability, in the moment)

- Unexpected attachment? Check the sender before you open.
- Look for the lock. Secure sites only.
- Urgent and unusual? That's the pattern. Slow down.
- Not sure? Hover first. Click second.
- A real supplier won't mind you checking.

Reporting (motivation, norms, safety)

- Odd email? One click. We'll check it, you carry on.
- Most of your team now report phishing within two hours.
- If something feels off, speak up. No blame.
- Thanks, we checked it. Reporting it was the right call.
- Finance reported 6 this week. Two were real.
- Reported in error? Still the right call. Thank you.
- Not sure it counts? Report it anyway. That's what we're here for.

Passwords and MFA (capability, enablement)

- Let the password manager remember it. You don't have to.
- MFA prompt you didn't trigger? Tap "No" and tell us.
- One password per site. The manager does the work.
- Prompt failing on your device? Tell us. We'll fix it, not you.

Leaders and managers (modelling)

- Report one yourself this week. Your team is watching.
- When someone reports, say thank you where the team can hear it.
- Ask "what's getting in your way?" before "did you complete it?"
- Share the near miss. No names. Just the lesson.

Onboarding and rhythm (embedding)

- Week one: here's what we do when something looks odd.
- Anything odd this week? One line in the stand-up.
- Security choices go in the retro with everything else.
- Your report stopped this. Here's what happened next.

Marcus's pack

Button label: "Odd invoice? One click. We'll check it, you carry on."

Reply: "Thanks, we checked it. Here's what we found. Reporting it was the right call."

Call-back step: "New bank details? Confirm by phone first. Protects the payment run."

Weekly channel line (true every time): "Finance reported 6 this week. Two were real."

Nothing with WARNING, must or failure in it.

Your one behaviour

Write three messages for your one behaviour: one at the moment of action, one reply or thank-you, one social-proof line that is true.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. **How does your current messaging feel: clear, supportive, overwhelming, or ignored?**

2. **Where could a well-timed nudge replace the need for repeated training?**

3. **Are you using fear or shame in your tone, or building trust?**

4. **What is one moment where a small message could make a secure behaviour easier?**

5. **Could you build a Cyber Message Pack for one team or one process?**

MODULE 5

Strategy Design for Human Risk

Key ideas from the video

- Behavioural objectives, not awareness goals: actions not attitudes, context-specific, visible and measurable, linked to real risk. Start small, then scale.
- Align with the business: risk register, audit findings, resilience KPIs, and translated language. "Fewer avoidable incidents", not "more awareness".
- Culture readiness: awareness, alignment, advocacy. Meet people where they are, then stretch. Ask for the next step, not the final destination.
- The Human Risk Strategy Framework has five parts and fits on one page: objectives, intervention design, culture levers, measurement and milestones, adaptation plan.
- Sustain it with rhythms, behaviour and story, feedback, visible modelling, and evolving together.

Template: behavioural objective builder

Vague version	Behavioural version (who, does what, by when, how often)
"We want people to be more security aware."	
"Improve the reporting culture."	
Your one behaviour:	

Check	Yes?
Describes an action, not an attitude	
Specific to a team and context, not generic	
Visible and measurable	
Linked to a named risk	
Small enough to start next month	

Template: business alignment

Behaviour	Risk register item or audit finding	Resilience or performance KPI it moves	The sentence leadership will hear

Behaviour	Risk register item or audit finding	Resilience or performance KPI it moves	The sentence leadership will hear

Template: culture readiness check

Tick the signals you actually observe. The stage with most ticks is where you are. Plan the next step from there.

Signal	Awareness	Alignment	Advocacy
How people talk about security	Rules, "they", compliance	"Part of the job", practical	"We", pride, stories
What happens after an incident	Blame or silence	Review, lessons, fixes	Shared openly, used to teach
Whether leaders model it	Rarely, or exempt themselves	Visibly, when asked	Unprompted, consistently
How teams treat secure action	Slows us down	Supported	Expected and recognised
Reporting	Low, late	Rising, faster	Routine, near misses included

Where we are	The realistic next step (not the destination)

Template: the one-page human risk strategy

1. Behavioural objectives: what exactly shifts, and why it matters

2. Intervention design: the layered actions, tailored to the COM-B diagnosis	3. Culture levers: rituals, language, leadership, norms

4. Measurement and milestones: success in behaviour, not policy	5. Adaptation plan: resistance, feedback, review dates

Where others can plug in

Template: rhythm planner

Rhythm	Cadence	Owner	What it reinforces
Behaviour check-in	Monthly		
Retro with security choices			
Recognition ritual			
Pulse or interview round	Quarterly		
Strategy review	30 / 60 / 90 days		

Marcus's one page

Objective: finance reports suspicious invoices within one hour; median today nine hours.

Business link: invoice fraud is risk 4 on the register; one near-miss this year worth £180,000.

Readiness: awareness stage, so safety and the manager's visible support come before any target.

Interventions: the five-layer stack; messages from module 4.

Measures: reports per week, median time to report, call-backs made, what the team says in the retro. Review at 30, 60 and 90 days.

How it landed: the CFO asked "what do you need from me?"; the finance manager co-signed it because it was written in her language.

Your one behaviour

Write your one page now, in pencil. It will change at thirty days, which is the point.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. **What specific behaviour do you want to change, and why?**

2. **Can you explain how that behaviour links to business or risk outcomes?**

3. **Where is your culture today: awareness, alignment or advocacy?**

4. **What would a one-page human risk strategy look like for your team or organisation?**

5. **How will you keep the strategy alive? What rhythms or rituals will help?**

MODULE 6

Embedding Change and Measuring Behaviour

Key ideas from the video

- Compliance metrics (training completed, policy accepted) miss the moments that stop breaches. Measure reporting, friction, help-seeking, follow-through and team language.
- A behaviour repeats when it has a cue, a routine and a reward. Most programmes design the routine and forget the reward.
- Do not add a security ritual. Put security inside the rituals that already exist: stand-ups, retros, onboarding, incident reviews, recognition, one-to-ones.
- Lagging indicators tell you what happened; leading indicators tell you what is about to. Three to five leading, one or two lagging. Measure at team level, never to surveil.
- Close the loop: collect, make sense, act, show people what changed.

Template: the habit loop for your behaviour

Cue (in the flow of work)	Routine (short enough under pressure)	Reward (lands within hours)

If the cue is not in the moment, the behaviour depends on memory. If the routine takes ten minutes, it loses to the deadline. If the reward arrives at the annual review, it never arrives.

Template: embedding in existing rhythms

Ritual that already happens	The one small change	Who makes it
Team stand-up	"Anything odd this week?"	
Retrospective		
Onboarding, week one		
Incident review		
Monthly update or all-hands		
Manager one-to-ones	"What is getting in your way?"	

Template: behavioural KPI set

Indicator	Leading or lagging	Baseline	Direction and target	Owner	Cadence

Marcus's set, with results at ninety days

Reports per week (leading): baseline 0; now 6 to 9 and holding.

Median time to report (leading): nine hours to under forty minutes.

Call-backs made on bank-detail changes (leading): every change, since week two.

Help requests and "does this count?" questions (leading): up, which is the point.

Fraud attempts caught (lagging): two genuine attempts stopped, one via the call-back.

Friction log: the button was missed on the mobile app; fixed in week five.

All measured at team level. Nobody is named in any report.

Template: feedback-loop planner

Collect (indicators, friction log, pulse questions, what people say)	Make sense (monthly, with the team)	Act (change one thing in the stack)	Show what changed (how and where people hear it)

Your one behaviour

Choose three leading indicators and one lagging for your one behaviour. Write the baseline today, even if it is zero.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. **Where are you reinforcing secure behaviour already, and where are the gaps?**

2. **What team rhythms (stand-ups, retros, onboarding) could embed behavioural reflection?**

3. **Are your current metrics telling you what people do, or just what they have signed off?**

4. **What would a useful behavioural feedback loop look like in your environment?**

5. **How will you keep evolving your strategy based on real signals and stories?**

MODULE 7

Leading Human-Centred Security

Key ideas from the video

- Leadership is influence, not position. People do not follow frameworks; they follow other people. Model it, lead with questions, build psychological safety.
- Influence without authority grows from credibility, trust and usefulness. Map your network, find shared goals, deliver value early. People listen to people who listen to them.
- If you do not shape the story of security, someone else will. Collect stories, frame them, tell them plainly, repeat them.
- Champions scale influence: recruit for trust, equip them with the tools in this workbook, give them a visible role, feed them back.
- The long-term change agent listens first, acts with empathy, and speaks the human language of security.

Template: influence map

Who trusts me now	What they care about (their goal, not mine)	Value I can deliver early	Who they could amplify me to

Template: story bank

Thirty-second stories: what happened, what it means, where to tell it. No names unless the person wants the credit. No blame, ever.

What happened	What it says about who we are becoming	Where and when to tell it
A developer paused a release because something felt off. It was a serious misconfiguration. No drama, no blame, just action.	We stop and check, and nobody gets punished for it.	Engineering all-hands; onboarding

Template: Champions network starter

Team	The person people already turn to	Visible role	Tools they get	How they hear what changed

Recruit for trust, not seniority. A Champion is not a deputy for the security team; a Champion carries the culture inside their own team.

Template: 30 / 60 / 90-day leadership plan

By day 30	By day 60	By day 90
One behaviour modelled visibly, every week	One story told in a forum that matters	One Champion in place with a role and a feedback loop

How Marcus scaled it, still without authority

Told the finance story in three sentences at the ops all-hands: two frauds stopped, no drama, no blame.

Asked each of the three teams who wanted the button for their Dee, then ran the grid and six coffees with them.

Gave the four Champions the interview guide and the message pack, and a monthly half-hour together.

Asked the finance manager to tell the story to her peers, not him.

Kept the strategy to one page: three teams, three behaviours, one measure each.

Your one behaviour

Who is the Dee for your one behaviour? Write their name, and the first thing you will ask of them.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. **What does human-centred leadership look like in your role, today?**

2. **Who trusts you now, and how could you build wider influence?**

3. **What story or ritual could help shift norms in your team or organisation?**

4. **What secure behaviour do you consistently model, or need to?**

5. **What is one step you will take to lead culture change, regardless of your job title?**

COURSE SUMMARY

Close

Seven ideas to carry forward

1. **Start with the context, not the tool.** Real life does not care about your framework. Map the forces that hold behaviour in place.
2. **Diagnose before you design.** Observe, interview, map. Tools do not fix a misdiagnosis.
3. **Layer, don't pile.** Nine functions. Match each to a barrier. Two or three, reinforcing each other.
4. **Communicate at the moment of decision.** Frame it, time it, say it like a human. Nudge, never manipulate.
5. **Make it a strategy the business owns.** Behavioural objectives, business language, culture readiness, one page.
6. **Embed it, measure it, close the loop.** Cue, routine, reward. Leading indicators at team level. Show people what changed.
7. **Lead from where you are.** Credibility, trust, usefulness, stories, and Champions to carry it.

The closing line

Real security begins when people feel safe enough to speak, strong enough to act, and supported enough to care.

One thing on Monday

Not the whole strategy. One thing: observe one team for an hour, have one diagnostic conversation, rewrite one message, tell one story. Write it here, with a date, and tell one other person.

Glossary

Term	Meaning
COM-B	Capability, Opportunity, Motivation leading to Behaviour. The diagnostic lens for what drives or blocks a behaviour.
Behaviour Change Wheel (BCW)	Nine intervention functions (education, training, persuasion, incentivisation, coercion, enablement, modelling, environmental restructuring, restriction) mapped to COM-B.
Context map	A picture of the pressures, friction, modelled behaviour and shadow systems around a behaviour. Study the system, not the person.
Behavioural Observation Grid	Structured record of what happened, where, who (role), what was said, and the likely COM-B driver. Behaviour as data.
Behavioural Diagnosis Map	Target behaviour at the centre; barriers and enablers under each COM-B branch; the dominant barrier marked.
Layering	Combining two or three intervention functions, each answering a diagnosed barrier, so they reinforce rather than overload.
Nudge	A small, transparent change to how a choice is presented that steers behaviour without removing it. Fails the test if it removes choice, shames or tricks.
Friction design	Adding friction to risky paths and removing it from secure ones so the system guides the decision.
Framing	How the same information is presented: gain or loss, social proof, timing. Changes what people do with it.
Behavioural objective	Who does what, by when, how often. An action, not an attitude; measurable; linked to a named risk.
Culture readiness	Awareness (know the rules, don't follow them), alignment (part of the job), advocacy (people champion it). Plan the next step, not the destination.
Leading / lagging indicator	Leading: a behaviour that predicts outcomes and moves in weeks. Lagging: the outcome itself (incidents, losses), months later.
Habit loop	Cue, routine, reward. The structure a behaviour repeats on; design all three.
Feedback loop	Collect, make sense, act, show what changed. The step that makes a strategy learn.
Psychological safety	The shared belief that it is safe to report, ask and admit mistakes. Without it, people act safely for themselves, which means silence.
Security Champion	A trusted colleague inside a team who carries the culture there. Recruited for trust, equipped, visible, fed back.

Further reading

- Michie, S., Atkins, L. and West, R. (2014). The Behaviour Change Wheel: A Guide to Designing Interventions. Silverback.
- Michie, S., van Stralen, M. M. and West, R. (2011). The behaviour change wheel. Implementation Science, 6(42). Open access.
- Thaler, R. H. and Sunstein, C. R. (2008). Nudge. Penguin.
- Service, O. et al. (2014). EAST: Four Simple Ways to Apply Behavioural Insights. Behavioural Insights Team. Open access.
- Edmondson, A. (2018). The Fearless Organization. Wiley.
- Kahneman, D. (2011). Thinking, Fast and Slow. Penguin.
- Clear, J. (2018). Atomic Habits. Random House.
- Wood, A. Building a Cybersecurity Culture; The Behavioural Change Playbook for Cybersecurity; The Rise of the Security Champion.

Notes