CYBEHAVE

Behavioural Risk Foundations

Course workbook

Understand, assess and influence human behaviour in cybersecurity.

Build Behaviour. Build Culture. Build Resilience.

This workbook belongs to

Organisation and role

Started on

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

BEFORE YOU START

How to use this workbook

The course is built to be a workshop, not a documentary. Every framework is designed to be applied immediately, 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, and the five Reflect & Apply questions with room to write.

Five ways to get the most from it

1. **Move at your own pace.** Pause, reflect, revisit. Behavioural science is absorbed in chunks with reflection between them, not in one sitting.
2. **Pick one behaviour and keep it.** Choose one behaviour in your own organisation that you would like to change, and run every framework in this course against that one behaviour. Each section has a "Your one behaviour" box for it. By module 6 you will have a working plan.
3. **Write, do not just think.** Retrieval, pulling an idea out of your head and onto the page, does more for retention than re-watching ever will.
4. **Apply as you go.** Do not wait for the end. When you meet COM-B in module 2, diagnose your behaviour with it that day.
5. **Bring an open mind.** Some of what follows challenges how the industry usually talks about people. A human lens reveals what a technical lens hides.

The course at a glance

Module	Title	You will be able to
0	Welcome	See the course as a whole, meet Sally, choose your one behaviour.
1	What is Human Cyber Risk?	Define human cyber risk and sort behaviours into errors, violations, habits and culture.
2	Behavioural Science Essentials	Diagnose a behaviour with COM-B instead of defaulting to "lack of awareness".
3	The Role of Culture and Norms	See the three kinds of norm at work and choose signals that shift them.
4	Identifying and Assessing Risky Behaviours	Look, listen and ask; prioritise by frequency, severity, exposure and changeability.
5	Influencing Behaviour the Right Way	Choose and combine interventions from the Behaviour Change Wheel.
6	Planning for Change	Write a behaviourally specific goal, sense-check with APEASE, build a one-page plan.
7	Embedding and Scaling Change	Measure behaviour not activity, pilot, iterate, embed, scale, and lead with trust.
8	Close	Carry the six big ideas forward; try one thing on Monday.

One idea we keep coming back to

Awareness is the entry point. Behaviour is the evidence of progress. Culture is where the future is built.

WORKED EXAMPLE

Meet Sally

Sally is a marketing manager at a mid-sized company: smart, ambitious, good at her job, juggling two or three live campaigns at a time. She is not careless and she is not stupid. She wants to do the right thing. She is busy, under pressure, and working in an environment that does not always make the secure path the easy path. Statistically, Sally is the median employee.

What we see Sally doing	Where it appears in the course
Reuses one password across about a dozen SaaS tools, to save time	Module 1: spotting the behaviours
Dismisses MFA prompts as "glitches"	Module 2: COM-B diagnosis
Ignores the report-suspicious-email button; does not want to bother IT	Module 5: choosing interventions
Forwards client briefs to her personal email at the weekend because the VPN is slow	Module 6: the 90-day plan
Clicked two suspicious links this year; both caught by IT, not her	Module 7: 90 days later
Skips the optional security training, as her manager does	

Use Sally as a mirror

Each time a Sally card appears in the video, ask: who is the Sally in my organisation for my one behaviour? What are they rushing to finish? What would make the secure path the easy path for them?

MODULE 1

What is Human Cyber Risk?

Key ideas from the video

- Human cyber risk is the likelihood that someone's actions, or inaction, will introduce threats to your systems, data or operations. No blame in the definition: the moment you start with blame you have prejudged the cause.
- Behaviour leads; errors, habits and culture all matter; the why matters more than the what; and human risk is measurable, changeable and worth investing in.
- Four types of risky behaviour: errors (accidental), violations (intentional workarounds), habits (unconscious patterns) and culture-driven (normalised practice). Each needs a different response.
- Most incidents start with a decision that felt harmless at the time. Risk lives in routines, not just in rare events.
- Knowing is not doing. Awareness is the entry point; behaviour is the evidence.

Template: the four-type sorter

List the risky behaviours you actually see in your team or organisation. Not the headline incidents: the everyday ones. Sort each into a type and note why. Expect to find that the dominant type is not the one your training budget targets.

Behaviour I see	Type (E / V / H / C)	Why I think so	Response it would need

E = error, V = violation, H = habit, C = culture-driven. Treat a habit like a violation and you get nowhere. Treat a violation like an error and it keeps coming back. Treat culture as an individual failing and you train one person and lose them to the team.

Template: how we respond to human error today

When someone...	What actually happens first	Curiosity, gratitude or blame?	What it teaches the next person
clicks a phishing link			
reports something that turns out to be nothing			
admits a mistake			
bypasses a control to hit a deadline			

Your one behaviour

Write your one behaviour as a first draft. You will sharpen it in module 6. For now: who does (or does not do) what, and roughly how often?

Reflect & apply

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

1. **What human risks do you see most often in your team or organisation?**

2. **Are they caused by mistakes, habits, workarounds, or cultural norms?**

3. **How does your organisation currently respond to human error?**

4. **Do you treat awareness as a proxy for behaviour, and is it working?**

5. **What one behaviour would you most like to change, and why?**

MODULE 2

Behavioural Science Essentials

Key ideas from the video

- We are feeling machines that think (Damasio). Emotion comes first; we decide fast and rationalise afterwards.
- System 1 is fast, automatic and runs most of the day, especially under pressure. System 2 is slow, deliberate and expensive. Cybersecurity is designed in System 2 but acted out in System 1.
- Habits form in a loop: cue, routine, reward. Every run without consequence strengthens it. To change a habit, change the loop.
- COM-B: behaviour needs Capability (physical and psychological), Opportunity (physical and social) and Motivation (reflective and automatic). If any one is missing, the behaviour will not happen.
- Diagnose first, then design. "Lack of awareness" is rarely the whole answer. If you trained everyone on Monday and nothing changed by Friday, Capability was not the only gap.

Reference: COM-B in one table

Component	Sub-type	What it means	Cyber examples
Capability	Physical	The practical ability to do the thing	Recognising the structure of a phishing URL; using the password manager extension
	Psychological	Knowledge, understanding, memory, focus, confidence	Understanding why MFA defeats credential theft; remembering the reporting procedure under pressure
Opportunity	Physical	External factors that make it possible, or annoying	Password manager pre-installed at onboarding; a report button in every email client
	Social	The people and culture around us	The manager visibly reports first; a reported mistake is met with thanks, not blame
Motivation	Reflective	Beliefs, values, intentions, reasoning	Believing reporting protects the team; valuing customer trust enough to slow down
	Automatic	Habits, instincts, emotional responses	A flicker of suspicion at an odd attachment; reflexively reaching for the password manager

Template: COM-B diagnosis of your one behaviour

For your behaviour, under real working conditions, score each sub-component: how strong is it now, what is the evidence, and how big is the gap? Resist defaulting to Capability. Spend twice as long here as feels natural.

Sub-component	What I observe (evidence, not assumption)	Gap: none / small / moderate / big
Physical capability		
Psychological capability		
Physical opportunity		
Social opportunity		
Reflective motivation		
Automatic motivation		

The weakest component, or the weakest pair, is:

Template: the habit loop

If your behaviour (or its insecure alternative) is a habit, map the loop as it runs today and as you would like it to run.

	Cue	Routine	Reward
Today			
Desired			

Worked example: Sally's diagnosis

Component	Finding	Gap
Capability	Can name phishing in training; does not recognise it in her inbox under deadline pressure	Moderate
Opportunity	Reporting takes four clicks; the team has never celebrated a catch	Big
Motivation	Her last report got "thanks, we'll look into it" and nothing came back	Big

The lesson: more training would address the smallest gap. The design has to make reporting one click and close the loop on every report.

Five tips for using COM-B

1. Diagnose first: find the actual barrier, not "lack of awareness".
2. Balance all three: skills, supportive systems and motivation together are what sustains.
3. Use social influence: peers, champions and positive norms move behaviour more than policy.
4. Fit the context: different roles have different barriers; one size never fits all.
5. Measure and refine: track changes in C, O and M and iterate. A system, not an event.

Further reading

Michie, S., van Stralen, M. M. and West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implementation Science, 6(42). Open access: doi.org/10.1186/1748-5908-6-42

Kahneman, D. (2011). Thinking, Fast and Slow. Penguin.

Reflect & apply

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

1. **Think of one insecure behaviour you have seen recently. Which part of COM-B was missing?**

2. **Is the behaviour driven by habit, pressure, or misunderstanding?**

3. **What environmental or cultural factors might be reinforcing the wrong behaviour?**

4. **How could you support Capability, Opportunity or Motivation in your context?**

5. **What is one thing you would do differently now when observing behaviour?**

MODULE 3

The Role of Culture and Norms

Key ideas from the video

- Culture eats strategy for breakfast. When the written strategy and the lived culture disagree, behaviour follows the culture.
- Security culture is the shared beliefs, norms and habits that shape how people make security decisions, especially when no policy is watching. It is revealed in action, shaped by leaders and peers, learned not taught, and built on trust.
- Three kinds of norm: descriptive (what people do), injunctive (what people believe they should do), subjective (what you think others expect). Change the norm and behaviour follows; change the rule and not much happens.
- The visible side (policies, completion rates, posters, audits) is what the board sees. The invisible side (quiet "don't worry about it", who reports and who doesn't, what "we" do when deadlines hit) is where the real risk lives.
- Four levers: model the behaviour; talk openly about mistakes; notice and recognise; match systems to values. Culture is built every day, in hundreds of small signals.

Template: norms audit for your one behaviour

Norm	As it is today (be honest)	As you want it to be	How you would make the change visible
Descriptive: what people actually do			
Injunctive: what people believe they should do			
Subjective: what people think others expect of them			

Template: visible and invisible

What our dashboard shows (visible)	What actually happens on a busy Tuesday (invisible)

What our dashboard shows (visible)	What actually happens on a busy Tuesday (invisible)

The exercise from the video: ask twenty people across different teams what they actually do when they are tired, late and a project is on fire. Whatever they tell you, that is your culture.

Template: four levers, one week

Lever	A signal I could send this week	Who sends it	By when
Model the behaviour			
Talk openly about mistakes			
Notice and recognise			
Match systems to values			

Your one behaviour

Which unwritten rule in your organisation most affects your one behaviour, and who are the three people whose example would move it?

Reflect & apply

Five questions, and they may be uncomfortable. That is normal.

1. **What is one unwritten rule in your organisation that shapes security behaviour?**

2. **Who are the most influential people on your team, and what do they model?**

3. **Is reporting met with curiosity, gratitude, or blame in your culture?**

4. **Where do your policies and your real-world norms disagree?**

5. **What small signal could you send this week to nudge culture in the right direction?**

MODULE 4

Identifying and Assessing Risky Behaviours

Key ideas from the video

- The first step toward change is awareness; the second is acceptance (Branden). Most assessment skips both: it measures compliance and calls it awareness.
- Risk hides in the ordinary: password reuse and sharing, clicking when distracted, not reporting, bypassing controls, oversharing on collaboration and AI tools, shadow IT. The biggest risks are routine, not dramatic.
- Look, listen, ask. You can't fix what you can't see, and you can't see what you don't make safe to share. Safety first, observation second.
- Prioritise by frequency, severity, exposure and changeability. Frequent, severe and changeable is your highest leverage. Pick the top three and do them properly.
- People support what they help identify. Co-design with the people doing the work, run workshops not just audits, empower champions, and share what changed.

Template: look, listen, ask

Mode	What I will do	With whom	By when	What I noticed
Look: watch the real workflow (tickets, walkthroughs, incident reviews)				
Listen: retros, corridors, informal channels				
Ask: short anonymous survey, curious 1:1s, open questions				

Template: prioritisation matrix

Score each behaviour 1 (low) to 5 (high). Multiply for a rough leverage score, then sanity-check the top three with the people closest to the work.

Behaviour	Frequency	Severity	Exposure	Changeability	Score

Behaviour	Frequency	Severity	Exposure	Changeability	Score

Template: co-design

Who could help identify the risks (team, role, champion)	How I will involve them (workshop, walkthrough, interview)	What I will feed back to them, and when

Your one behaviour

For your one behaviour: how often does it really happen, who has access to what when it does, and what is the smallest workflow change that would move it?

Reflect & apply

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

1. **What is a "normal" behaviour in your organisation that quietly introduces risk?**

2. **How well do you actually understand what your front-line teams do day to day?**

3. **Where do you observe, and where do you only audit?**

4. **If you prioritised by frequency x severity x changeability, what would top your list?**

5. **Who could you co-design with to make your next assessment more honest?**

MODULE 5

Influencing Behaviour the Right Way

Key ideas from the video

- If you want to encourage some activity, make it easy (Thaler). Apply the test to every intervention: does this make the desired behaviour easier, not just more convincing?
- Four principles: match the barrier (diagnose with COM-B first), combine rather than isolate, ethical first (no dark patterns, no fear-only messaging), test and learn.
- The Behaviour Change Wheel gives nine intervention types. Most programmes use two or three. There is unused leverage lying on the shelf.
- Environmental restructuring is the most underused and highest-leverage intervention. Coercion kills reporting and belongs at the tail of a graduated response. Recognition beats money; frequency beats magnitude; specificity beats vagueness.
- Sally's stack: one-click reporting (environmental restructuring), the manager reports first (modelling), every report gets a reply (enablement), a 15-minute refresher (light training). Friction down, meaning up.

Reference: the nine interventions

Intervention	What it is	COM-B target	Cyber examples
Education	Increasing knowledge or understanding	Capability (psychological)	Phishing content with real examples; short explainers on why MFA works
Persuasion	Communication that shifts feelings or stimulates action	Motivation	Peer stories of catching a phish; framing reporting as protecting colleagues
Incentivisation	Creating an expectation of reward	Motivation	Recognition for first-time reporters; team shout-outs for reporting rate
Coercion	Creating an expectation of consequences (sparingly, ethically)	Motivation (reflective)	Lockout after repeated MFA bypass; formal consequences for proven repeat violations
Training	Imparting skills through guided practice	Capability	Hands-on simulations with feedback; password manager practice at onboarding
Restriction	Rules that reduce the opportunity for the unwanted behaviour	Opportunity (physical)	Blocking unsanctioned file sharing; macros off by default; least privilege
Environmental restructuring	Changing the physical, digital or social context	Opportunity	One-click report button; password manager pre-installed; external-sender banners
Modelling	Providing an example to imitate	Motivation (automatic) and social Opportunity	Leaders visibly reporting; Champions demonstrating in team rituals

Intervention	What it is	COM-B target	Cyber examples
Enablement	Increasing means or reducing barriers	All three	A help desk that answers without judgement; coaching on tricky workflows

Reference: from COM-B gap to intervention

Gap	Look first at
Capability	Education, Training, Enablement
Opportunity	Restriction, Environmental restructuring, Enablement
Motivation	Persuasion, Incentivisation, Modelling, Coercion (last resort)

Template: your intervention stack

Two or three interventions, mapped to the gaps you diagnosed in module 2, that reinforce each other. For each, apply Thaler's test.

COM-B gap it targets	Intervention type	What it would actually look like here	Does it make the behaviour easier? (yes / no / how)

Template: who could model it?

Person credible to this audience	What they would be seen doing	Where it would be visible (channel, ritual)	How often

Person credible to this audience	What they would be seen doing	Where it would be visible (channel, ritual)	How often

Reflect & apply

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

1. **Pick one behaviour you want to change. What is its main barrier: C, O or M?**

2. **Which two BCW interventions would you combine to address it?**

3. **Where could you replace "more training" with "less friction" (environmental restructuring)?**

4. **Who could model the behaviour, and how could you make their actions visible?**

5. **How would you measure whether your intervention is actually shifting behaviour?**

MODULE 6

Planning for Change

Key ideas from the video

- Plans are nothing; planning is everything (Eisenhower). Invest in the planning discipline so you can adapt when reality arrives.
- Start with the behaviour, not the tool. Who, does what, when, in what context, to what standard. Vague goals ("improve awareness") cannot be diagnosed, designed for or measured.
- Four steps: diagnose with COM-B; design by mapping gaps to BCW interventions; sense-check with APEASE; bring it together on one page.
- APEASE: Affordability, Practicability, Effectiveness, Acceptability, Side-effects, Equity. Not every clever idea survives, and that is the point.
- A plan beats a wish. A reviewed plan beats both. Pilot the smallest version with one team in two weeks.

Template: the behaviour statement

Slot	Your answer
Who	
Does what (observable)	
When	
In what context	
To what standard (how often, how fast, by when)	

Written as one sentence:

Example: "Marketing team members report suspicious emails within 60 minutes of receiving them, at least 80% of the time, within 90 days."

Template: APEASE sense-check

Score each intervention in your stack. Drop anything that fails decisively; adapt anything that fails marginally.

Criterion	Question	Score 1-5	Notes and how to strengthen
Affordability	Can we realistically resource it with the budget and people we have?		
Practicability	Can it be delivered as designed, not just as slides?		
Effectiveness	Is there evidence it will move the behaviour, or are we guessing?		
Acceptability	Will leadership, employees and users live with it day to day?		
Side-effects	Could it suppress reporting, push behaviour to shadow IT, create perverse incentives?		
Equity	Does it work fairly across roles, abilities, languages and working patterns?		

Template: the one-page plan

Question	Your plan
1. Target behaviour: who does what, when, in what context, to what standard?	
2. Current state: how often does it happen now? Where doesn't it? What is the baseline?	
3. COM-B diagnosis: which component, or combination, is the gap?	
4. BCW interventions: which one to three types address the gap?	
5. APEASE check: what passed, what was adapted, what was dropped?	
6. Owners and timing: who is responsible for each part, by when, with what support?	
7. Success metrics: how will you measure behavioural change, not just activity?	
8. Review and iterate: when will you review and adapt? (30 / 60 / 90 days)	

Worked example: Sally's 90-day plan

Element	Plan
Target behaviour	Marketing team members report suspicious emails within 60 minutes, at least 80% of the time, within 90 days
Current state	About 8% reported; average time-to-report over a day
Diagnosis	Opportunity and Motivation gaps dominate; Capability secondary
Interventions	Environmental restructuring (one-click button in Outlook); Modelling (marketing lead reports first, weekly); Enablement (every report gets a 24-hour outcome reply); light Training (15-minute refresher on real inbox patterns)
APEASE	Affordable and practicable with current tools; strong evidence; high acceptability because friction is removed; minor misclick risk monitored; works across the whole team
Metrics and review	Report rate (primary), time-to-report, satisfaction with the feedback loop; review at 30, 60 and 90 days
Owners	Security team: button rollout. Marketing lead: modelling. Security operations: feedback loop. Marketing champion: refresher

Template: the smallest first step

Pilot team	What we will try	Start date	What we will measure	Two-week check-in date

Reflect & apply

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

1. **Pick one behaviour you want to change. Can you write it in the "who does what, when, where" form?**

2. **Where is the COM-B gap: Capability, Opportunity, or Motivation?**

3. **Which 2 or 3 BCW interventions would you combine to address it?**

4. **Run your draft plan through APEASE. Which letter is weakest, and how could you strengthen it?**

5. **What is the smallest first step you could pilot in the next two weeks?**

MODULE 7

Embedding and Scaling Change

Key ideas from the video

- Awareness gets attention. Behaviour gets results. Culture gets durable. Build all three, in sequence.
- Measure outcomes, not outputs. Activity metrics (completion rates, emails sent, hours delivered) say something happened. Behavioural metrics (report rate by team, time-to-report, password manager usage, confidence under pressure) say whether anything changed. Measure at team level: this is about understanding behaviour, never about surveilling individuals.
- Universal goals, local design: segment by role and risk, adapt the medium, localise the message, reuse rituals that already exist.
- Five phases: pilot small, measure honestly, iterate, embed, scale. Behaviour change is a flywheel of small wins compounded, not a campaign.
- Lead with trust, not fear: thank, don't blame; share what changed; lead with humility; treat people as partners. Psychological safety is the soil all good security cultures grow in.

Template: swap activity metrics for behavioural metrics

Activity metric we report today	Behavioural metric that would show real change	Where the data would come from	Team-level, never individual?

Template: segment and localise

Audience segment	Their main COM-B barrier	The local "why" that lands with them	Medium and ritual to use
Executives			

Audience segment	Their main COM-B barrier	The local "why" that lands with them	Medium and ritual to use
Developers / technical			
Customer-facing			
Contractors / new starters			

Template: five-phase tracker

Phase	What done looks like	Status	Date	Notes
1. Pilot small	One team, one behaviour, short window			
2. Measure honestly	Behavioural metrics tracked and shared, including what is not working			
3. Iterate	Interventions tuned from data and from what people say			
4. Embed	Built into onboarding, rituals, tool defaults, workflow checkpoints			
5. Scale	Rolled out to other teams, adapted not copy-pasted			

Template: the trust audit

Act of leadership	What happens in our organisation today	What I will do differently this month
Thank, don't blame		
Share what changed		
Lead with humility		
Treat people as partners		

Template: 30 / 60 / 90-day review

Review	Primary metric (now vs baseline)	What the people say	What we will change	Owner
30 days				
60 days				
90 days				

Reflect & apply

The last reflection of the course. These matter most, because they are about how you will lead.

1. **Which behavioural metric would best tell you whether your culture is shifting?**

2. **Where could you pilot small instead of launching big?**

3. **What ritual or rhythm already exists in your organisation that you could piggy-back on?**

4. **How do you currently respond to mistakes, and is that response building or eroding trust?**

5. **What is one small leadership signal you could send this month to model the change?**

MODULE 8

Close: carry it forward

Six ideas that summarise the course

1. **Human risk is the biggest cyber risk.** And it is measurable, changeable and worth investing in.
2. **Behaviour follows COM-B.** Capability, Opportunity and Motivation explain why people act, or don't. Diagnose first.
3. **Culture is what people do.** Built every day, in small signals, more than in policies.
4. **Diagnose before designing.** Observe and assess what is really going on, then prioritise by impact.
5. **The Behaviour Change Wheel gives you nine levers.** Match interventions to the diagnosed barrier, and combine them.
6. **Pilot, measure, embed, scale.** Lead with trust. Behaviour change is a flywheel, not a campaign.

One thing on Monday

Not the whole plan. One thing, with one team, that you can start in the next week. Write it here, with a date, and tell one other person.

Glossary

Term	Meaning
Human cyber risk	Risk arising from human behaviour or inaction: errors, habits, workarounds, cultural norms.
COM-B	Capability, Opportunity, Motivation leading to Behaviour. Diagnostic framework for what drives or blocks behaviour.
BCW	Behaviour Change Wheel. Nine intervention functions for shifting behaviour, mapped to COM-B.
APEASE	Affordability, Practicability, Effectiveness, Acceptability, Side-effects, Equity: the sense-check filter for interventions.
Security culture	Shared beliefs, norms and habits that shape how people make security decisions, especially when unobserved.
Norms	Descriptive (what people do), injunctive (what they should do), subjective (what they think others expect).
Psychological safety	The shared belief that the team is safe for interpersonal risk-taking: admitting mistakes, asking questions, reporting.
Nudge	A small change to the choice environment that gently steers behaviour without restricting choice.
Modelling	Providing an example for people to aspire to or imitate.
Behavioural metric	A measure of what people actually do (for example, report rate), distinct from activity metrics (for example, training completion).
System 1 / System 2	Fast, automatic, pattern-matching thinking versus slow, deliberate, effortful thinking (Kahneman).
Habit loop	Cue, routine, reward. The structure a habit runs on, and the structure you change to change the habit.

Further reading

- Michie, S., van Stralen, M. M. and West, R. (2011). The behaviour change wheel. Implementation Science, 6(42). Open access.
- Michie, S., Atkins, L. and West, R. (2014). The Behaviour Change Wheel: A Guide to Designing Interventions. Silverback.
- Kahneman, D. (2011). Thinking, Fast and Slow. Penguin.
- Thaler, R. H. and Sunstein, C. R. (2008). Nudge. Penguin.
- Damasio, A. (1994). Descartes' Error. Putnam.
- Edmondson, A. (2018). The Fearless Organization. Wiley. (Psychological safety.)
- Verizon Data Breach Investigations Report, published annually.

Notes