PRIMER

Secure Behaviour Management 101

Secure Behaviour Management (SBM) explained: its origin, how it differs from awareness training and human risk management, and where Security Champions fit.

IN THIS DOCUMENT

Where the term came from	2
How it compares	2
Why awareness is not enough	3
The core ideas	4
Four things the industry gets wrong	5
What it involves	5
Where Champions fit	6
Management is not surveillance	7
Questions	7
Glossary	8
Go deeper	8

Built on 22 November 2026 from the live page at
cybehave.com/secure-behaviour-management

What is Secure Behaviour Management?

> **Secure Behaviour Management (SBM)** is the practice of defining, measuring and improving the everyday behaviours that keep an organisation secure. It judges a programme by whether people act more securely than they did before, and whether that change can be shown, not by how many people completed a course.

The term is new in 2026. The problem it names is not. This page explains where the name came from, how it relates to security awareness and human risk management, the handful of ideas you need to know, and why we think Security Champions are how it gets delivered through people.

Where the term came from

Gartner began using the name Secure Behavior Management during 2026. One of the first papers to carry it was Wam Voster's Implement Secure Behavior Management to Secure Your Cyber-Physical Systems, published in July 2026, which applies the idea to factories, utilities and other industrial sites. Its starting point is that the most common exposure in those environments is an ordinary human decision, such as a technician sharing credentials because changing them feels disruptive.

The paper sets out five components: training built around each role, local security ambassadors at each site, scenario exercises that reflect real operations, coverage of contractors and suppliers, and measures tied to operational outcomes in place of completion counts. The second matters most to us. Gartner describes ambassadors as local people with operational credibility, often with no security background, who translate central policy into local terms and escalate what they see. So one of the earliest Gartner papers on the subject places Security Champions inside Secure Behaviour Management.

The name has since been applied more broadly. Keepnet reports that a Gartner note in September 2026 uses it for the whole market previously called security awareness training, and in the UK SASIG ran a session on it the same month. You will also see the science underneath it called behavioural cybersecurity. The idea is older than the label: security teams have spent years discovering that people who know the rules still break them, usually for sensible local reasons. SBM gives that problem a name that points at the thing to be changed.

One problem, four names

Each name the industry has used asks a slightly harder question than the one before. The tools overlap a great deal. What changes is what counts as success.

NAME	THE QUESTION IT ASKS	WHAT IT TENDS TO MEASURE
Security awareness training (SAT)	Has everyone been told?	Course completion and phishing click rates
Security behaviour and culture programme (SBCP, Gartner's earlier term)	Are we building a culture as well as running a course?	Culture surveys and behaviour indicators
Human risk management (HRM, used by Forrester and many vendors)	Which people carry the most risk, and how do we reduce it?	Risk scores for each person
Secure Behaviour Management (SBM, Gartner, 2026)	Do people behave more securely than they did, and can we show it?	The same behaviours, before and after

Human risk management and Secure Behaviour Management cover much the same ground, and buyers will meet both for some time. We prefer the newer name because it describes what you want more of. People are far easier to work with when they are not introduced as the risk.

Why awareness is not enough

Phishing, business email compromise and MFA fatigue attacks all work the same way: they target a decision, not a device. They use urgency, authority and familiarity to catch people in the fast, automatic mode of thinking that runs most of our day[3,11]. The attacker is not exploiting a lack of knowledge. They are exploiting how attention works.

2 in 3

Roughly two thirds of breaches involve a human element: an error, a stolen credential, a manipulated decision[1]. **A defence that only addresses the technical third is defending a minority of the problem.**

The obvious response, "train people harder", has been tested for decades. Awareness campaigns raise knowledge scores and leave behaviour largely unchanged[10], because what people intend to do and what they do are only weakly linked[4]. Blaming people does not help either. One of the founding papers of the field showed that people behave insecurely largely because security is designed without them in mind[2], and non-compliance is often a rational response to rules whose cost outweighs their visible benefit[7]. Fix the design and the behaviour follows.

Awareness asks **"do people know the right thing?"** SBM asks **"do people do the right thing, and if not, why not?"** Being clear about which level you are working on changes what you do and what you measure.

LEVEL 1

Awareness

"Do people know?"

Knowledge of threats, policies and correct responses. Necessary, cheap to deliver and easy to measure with a quiz. On its own it changes very little.

LEVEL 2

Behaviour

"Do people do it?"

Observable actions: reporting a suspicious email, challenging an unexpected request, locking a screen. This is where risk changes, and it has to be measured directly.

LEVEL 3

Culture

"Is it just how we do things here?"

Shared norms and unwritten rules that make secure behaviour the default when nobody is watching[14]. Culture is what sustains behaviour after the campaign ends.

The ideas that explain most security behaviour

You do not need a psychology degree. **Start with the model that ties everything together.** The COM-B model, from the Behaviour Change Wheel, says any behaviour requires three things at once: the capability to do it, the opportunity to do it, and the motivation to do it[5]. If a behaviour is not happening, at least one is missing. Training only ever addresses the first.

C

Capability

Do they know how, and can they physically and mentally do it? Skills, knowledge, attention.

O

Opportunity

Does the environment allow it? Time, tools, workload, and whether the people around them do it too.

M

Motivation

Do they want to, in the moment? Habits, emotions, beliefs about consequences, identity.

COGNITION

Fast and slow thinking

Most decisions are made quickly and automatically, and attacks are built to keep you in that mode[3].

So what: Make the secure choice the obvious one, and add a deliberate pause only where it matters.

COGNITION

The intention-action gap

People who fully intend to behave securely frequently do not[4].

So what: Stop treating quiz scores and pledges as behaviour. Measure what people do.

EFFORT

The compliance budget

People hold a finite reserve of time and effort for security. Once it is spent, corners get cut[6].

So what: Every new control has a cost. Remove low-value demands before adding more.

EFFORT

Security fatigue

Bombarded by warnings and decisions, people stop reading and default to whatever is easiest[8].

So what: Fewer, better-timed messages beat constant noise.

EFFORT

Shadow security

When official controls get in the way, people invent workarounds that show exactly where the design fails[9].

So what: Treat workarounds as diagnostic data. Ask why before you ban.

SOCIAL

Social norms

People take their cues from what others around them do far more than from what a policy says[11].

So what: Make good behaviour visible. Security Champions move norms in ways broadcast messages cannot.

SOCIAL

Psychological safety

People report mistakes and near misses only when they believe they will not be punished for it[13].

So what: Reporting rate is a culture signal. Silence does not mean nothing is happening.

ENVIRONMENT

Defaults and friction

The way a choice is presented shapes the choice. Defaults are sticky, and a little friction goes a long way[12].

So what: Make the secure path the easy one. See choice architecture.

Four things the industry gets wrong

"Humans are the weakest link."

People are the most adaptive control you have, and the only one that can spot something the rules did not anticipate. **Poorly designed security is the weak link.** The person is where it shows[2].

"Phishing click rate tells us how secure we are."

Click rate measures one behaviour, under one set of conditions, with a simulated lure. **Measure a small set of behaviours that matter, including reporting**, which matters more.

"Punishing repeat clickers fixes the problem."

Punishment suppresses reporting. People stop telling you what happened[13]. **You trade a visible problem for an invisible one.**

"Annual training covers it."

One-off events produce a short-lived knowledge bump and no lasting change in behaviour[10]. **Behaviour change is continuous work**, done in small, measured cycles.

What Secure Behaviour Management involves

Strip away the product language and an SBM programme does four things, in this order. Treat it as an experiment, not a campaign.

01

Name the behaviours

Choose a small number of observable actions that matter in your organisation: reporting a suspicious message, verifying a payment change on a known number, challenging an unusual request from someone senior.

02

Measure where you are

Find out how often those behaviours happen today, team by team. Without a baseline, nothing that follows can be shown to have worked.

03

Change the conditions

Make the secure action easier, more normal and better supported. That can mean redesigning a process, a prompt at the right moment, or a trusted colleague showing how it is done.

04

Show the change

Measure the same behaviours again and report the difference. This is the evidence a board, an auditor or a regulator can use.

The full method. The SHIELD framework is the same loop in six stages: Specify, Hypothesise, Intervene, Embed, Learn, Diffuse. It adds the two things four steps leave out: working out why a behaviour is not happening before you try to change it, and carrying what worked to the next team.

A note on measurement. The most common failure in this field is measuring the wrong thing. Training completion, quiz scores and campaign reach tell you what the security team did, not what the organisation does. Measure behaviour directly, keep separate signals separate, and measure repeatedly so you can see change, not a snapshot.

Where Security Champions fit

Most descriptions of SBM are written one employee at a time: a nudge for each person, training chosen for each person, a score for each person. That is useful, and it leaves something out. People adopt a security behaviour mainly because the people around them do it.

Research on how behaviour spreads shows that information passes on a single contact, while a behaviour that costs effort or carries social risk usually needs reinforcement from several people before it sticks. We cover the evidence in Simple and Complex Contagion and what it means for coverage in The Champion Density Problem.

A Security Champion is a trusted colleague who makes the secure action the normal one in their team. A Champions Network connects those people so the behaviour can travel across the organisation and be measured as it goes. In our view that makes Champions the delivery mechanism for Secure Behaviour Management, working alongside whatever software you use.

Behaviour seen by colleagues

Heroes measures what people observe happening around them in their team. It reports patterns, and it does not track individuals.

Coverage and connection

See which teams have a Champion, which have nobody, and how security influence moves between them.

Evidence a board can use

Before and after measures of behaviour, network strength and programme capability, in plain language.

Management is not surveillance

Adapting a programme to what each employee did means keeping a record of what each employee did. Handled carelessly, that becomes monitoring under a friendlier name, and staff notice. Once people believe their mistakes are being logged against them they stop owning up, which removes the most valuable security behaviour of all.

Our position is that secure behaviour should be measured at the level where it lives, which is the team. CyBehave measures and informs. It does not surveil.

People, and now AI agents

One advantage of the new name is that it does not say "human". AI agents now act on our behalf, reading instructions literally and repeating them at scale, so whether an agent behaves securely is becoming a practical question for every security team.

Behavioural Convergence Theory is our research into whether the behavioural science used for people can be extended to understand and govern agents. If it can, Secure Behaviour Management is one discipline covering both.

Questions about Secure Behaviour Management

What is Secure Behaviour Management?

Secure Behaviour Management (SBM) is the practice of defining, measuring and improving the everyday behaviours that keep an organisation secure. It judges a programme by whether people act more securely than they did before, and whether that change can be shown, not by how many people completed a course.

Is Secure Behaviour Management the same as human risk management?

They describe much the same market and many of the same tools. The difference is the starting point. Human risk management treats people as a risk to be measured and reduced. Secure Behaviour Management names the behaviour you want to see more of and manages towards it.

Does Secure Behaviour Management replace security awareness training?

It changes what training is for. Regulators and auditors still expect training, so it does not disappear. Under SBM, completion stops being the headline measure and training becomes one of several ways to change a specific behaviour. Our Beyond Awareness page covers the move in more detail.

How do you measure secure behaviour?

Pick a small number of observable behaviours, such as reporting a suspicious message or verifying a payment change on a known number, and measure them before and after an intervention. Useful measures include how often and how quickly people report, what colleagues observe happening in their team, and whether the behaviour is spreading from team to team. Keep each signal separate; do not blend them into a single score.

Where should an organisation start with Secure Behaviour Management?

Pick one or two specific behaviours that matter, establish a baseline, understand why people currently do or do not perform them, design an intervention that addresses that reason, and measure the change. The SHIELD framework describes this as six stages: Specify, Hypothesise, Intervene, Embed, Learn, Diffuse.

Where do Security Champions fit in Secure Behaviour Management?

Security Champions are how secure behaviour reaches teams through people. Most security behaviours are adopted because trusted colleagues do them, so a connected network of Champions gives an SBM programme the peer reinforcement that software nudges alone cannot provide.

Is it Secure Behaviour Management or Secure Behavior Management?

Both are the same thing. Gartner and most US vendors write Secure Behavior Management. UK and Commonwealth organisations write Secure Behaviour Management. The abbreviation SBM is used for both.

Terms you will meet

Behaviour change technique (BCT)

A specific, replicable component of an intervention, such as goal setting, prompts or feedback[5]. Not to be confused with Behavioural Convergence Theory, CyBehave's own framework, which shares the abbreviation.

Choice architecture

The design of the environment in which people make decisions: defaults, ordering, friction, framing[12].

COM-B

A model stating that behaviour requires Capability, Opportunity and Motivation at the same time. The diagnostic core of the Behaviour Change Wheel[5].

Nudge

A small change to choice architecture that steers behaviour without removing options[12]. Useful for simple, repeated behaviours; not enough on its own for complex ones.

Security Champion

A member of a business team who acts as a local advocate and point of contact for security. Champions shift social norms because they are peers, not the security department.

Security culture

The shared assumptions, values and practices that shape security behaviour in an organisation, especially when nobody is watching[14].

Go deeper

SHIELD

The six-stage framework

An open method for running behaviour change as a discipline.

cybehave.com/science#shield

The Science

Why cybersecurity is a human science

The research behind the ideas on this page.

cybehave.com/science

Security Champions

Putting norms to work

Why peer-led programmes move behaviour that broadcast messages cannot.

cybehave.com/champions

Skills Framework

What practitioners need to know

Seven domains and thirty competencies for behavioural security work.

cybehave.com/science#skills

References

1. Verizon (2024) *Data Breach Investigations Report*. Verizon Business.
2. Adams, A. and Sasse, M.A. (1999) 'Users are not the enemy', *Communications of the ACM*, 42(12), pp. 40–46.
3. Kahneman, D. (2011) *Thinking, Fast and Slow*. London: Allen Lane.
4. Sheeran, P. (2002) 'Intention–behavior relations: a conceptual and empirical review', *European Review of Social Psychology*, 12(1), pp. 1–36.
5. 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.
6. Beautement, A., Sasse, M.A. and Wonham, M. (2008) 'The compliance budget: managing security behaviour in organisations', *Proceedings of the New Security Paradigms Workshop (NSPW)*, pp. 47–58.
7. Herley, C. (2009) 'So long, and no thanks for the externalities: the rational rejection of security advice by users', *Proceedings of the New Security Paradigms Workshop (NSPW)*, pp. 133–144.
8. Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S. (2016) 'Security fatigue', *IT Professional*, 18(5), pp. 26–32.
9. Kirlappos, I., Parkin, S. and Sasse, M.A. (2014) 'Learning from “shadow security”: why understanding non-compliant behaviors provides the basis for effective security', *Proceedings of the Workshop on Usable Security (USEC)*.
10. Bada, M., Sasse, M.A. and Nurse, J.R.C. (2015) 'Cyber security awareness campaigns: why do they fail to change behaviour?', *Proceedings of the International Conference on Cyber Security for Sustainable Society*, pp. 118–131.
11. Cialdini, R.B. (2007) *Influence: The Psychology of Persuasion*. Revised edn. New York: Harper Business.
12. Thaler, R.H. and Sunstein, C.R. (2008) *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New Haven: Yale University Press.
13. Edmondson, A. (1999) 'Psychological safety and learning behavior in work teams', *Administrative Science Quarterly*, 44(2), pp. 350–383.
14. Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behavior: a practice perspective', *Computers & Security*, 98, 102003.

Sources on the term

- Gartner, Implement Secure Behavior Management to Secure Your Cyber-Physical Systems, Wam Voster, 9 July 2026, G00856856 (client access).
- Keepnet, What is secure behaviour management?, October 2026. A vendor account of Gartner's September 2026 research.
- SASIG, Your Guide to Secure Behaviour Management, webinar, 16 September 2026.
- Forrester, Four Things You Should Know About Security Champions Networks, 2026.
- CyBehave, Secure Behaviour Management: right name, wrong unit. Our view on the change of name.

Gartner's research is available to its clients only. This page summarises the July 2026 paper in our own words. Its description of Gartner's September 2026 research relies on vendor accounts and should be read with that in mind.

About this document

This document was built on 22 November 2026 from the page at cybehave.com/secure-behaviour-management, so it carries the guidance as it was published that day. The page is kept up to date; download a fresh copy whenever you need one.

This page **cybehave.com/secure-behaviour-management**

Free Champions Programme Health Check **cybehave.com/champions-health-check/**

The Rise of the Security Champion, free ebook **cybehave.com/the-rise-of-the-security-champion**

HEROES by CyBehave, free 28-day trial **cybehave.com/trial**

© 2026 CyBehave Ltd. You are welcome to share this document with colleagues. Please keep it whole and credit CyBehave.