MODELS

Network models for Security Champions

Five network models for a Security Champions programme, the difference between spreading information and behaviour, and why where champions sit matters most.

IN THIS DOCUMENT

Two kinds of spread	2
Five models	3
Cluster or clustered	6
Reference model	7
The journeys	9
Where Heroes fits	10
Glossary	10

Coverage is a spreadsheet. Reach is a network.

Most Security Champions programmes are designed as rosters: how many champions, which teams, what they will be asked to do. How the champions are connected, to each other and to the colleagues sitting beside them, gets treated as admin. It is the main design variable. What a champions network can carry depends on its shape, and the shape that spreads information is not the shape that spreads behaviour.

A champions network is asked to spread two different things.

Network science has spent twenty years separating two ways things move through a social network. **Simple contagion** travels on a single exposure: you hear that a new phishing lure is doing the rounds, and the hearing is the whole transmission. **Complex contagion** needs reinforcement: a person adopts a behaviour only after several of the people around them have, and the several has to be visible at the same time.

Awareness, alerts and know-how behave like the first. Reporting a suspicious message, pausing on a request that arrives with authority attached, or changing a working habit behave like the second. A programme is asked to do both, and the two jobs pull the network design in opposite directions.

SIMPLE CONTAGION

Information

One exposure can be enough. The ideal network has many long ties, short paths and low redundancy, and the ideal seeds are the people who sit on the bridges between groups.

- A live threat alert reaching every team
- Where and how to report
- What a new policy or tool is for
- What a deepfake voice call sounds like

COMPLEX CONTAGION

Behaviour

A single long tie into a new team cannot carry it, because the person at the far end sees only one adopter. It needs clustered neighbourhoods, where a person's contacts also know each other, and wide bridges between them.

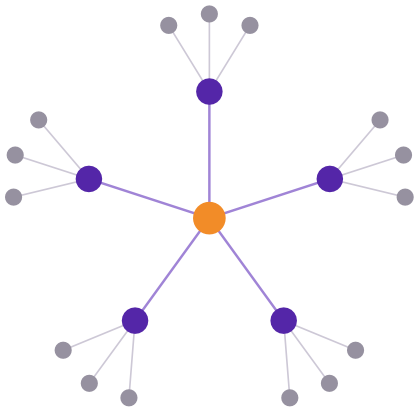
- Reporting routinely, including the false alarms
- Pausing on an urgent request from someone senior
- Using the password manager; no more shared credentials
- Holding a rehearsed response under pressure

Four things make a behaviour complex, and all four are common in security: it costs something; its value depends on others doing it too; it risks looking foolish; and it conflicts with a habit. A network designed for the top of this list fails quietly at the bottom, and the failure does not show in the usual metrics, because champions recruited, attendance and content delivered are all measures of simple contagion.

Five network models, and what each one can carry

Having run one network and advised on many, we can recognise five recurring shapes. Real programmes are usually a mixture, but each has a distinct profile against the properties that matter for contagion: path length, clustering around colleagues, ties among champions, the width of the bridges between teams, and what happens when someone leaves. Find the one you have built.

Champion Lead champion Colleague Security function



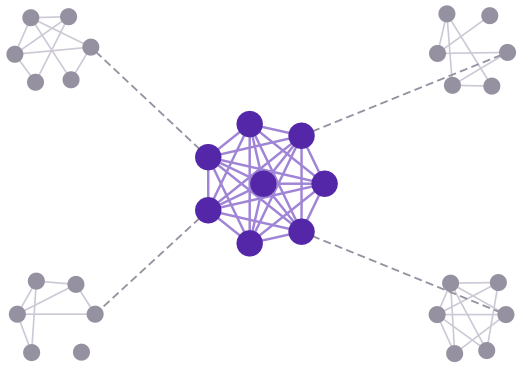
MODEL 1

Hub and spoke

Carries information outward · Carries no behaviour · Fragile

The default when a programme is launched from a mailing list. Each champion is tied to the centre, receives material and is expected to pass it on. Champions rarely know one another. Cheap to run, easy to measure, and a good carrier of alerts: every team is two hops from the security function.

It carries almost nothing back, and no behaviour at all, because each champion is a single adopter in a team of non-adopters and can supply only one signal. A champion who leaves takes their spoke with them; a centre that loses attention loses the network.



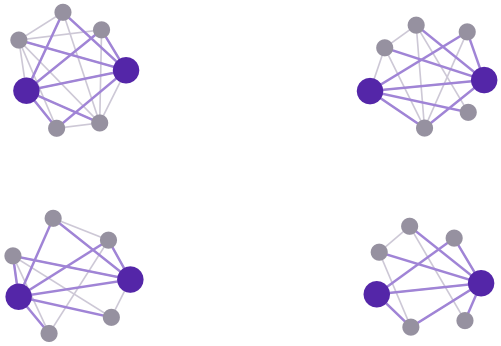
MODEL 2

A single champion cluster

Fast information among champions · Behaviour spreads among champions only · Runs parallel to the business

The model programmes grow into. The champions get a channel, a regular call and events of their own, and over a year or two they become a community of practice. Measured on its own terms it is a success: the champions know more, stay longer and speak up more.

The difficulty is where the ties are. Most of a champion's security-related ties now run to other champions. **The dense, reinforcing structure that behaviour needs has been built among the people who have already adopted.** From a colleague's desk the champion is still one adopter among non-adopters, and the cluster is somewhere else.



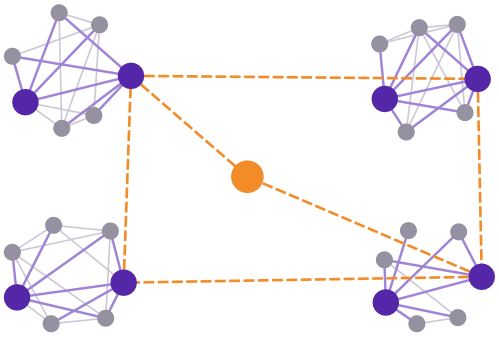
MODEL 3

Distributed champions, embedded in teams

Carries behaviour within teams · Information moves slowly · Isolation and drift

Champions sit inside the teams whose behaviour is to change, chosen for their position in the team rather than their interest in security, and placed in twos or threes so a colleague can see more than one adopter at once. Few ties between champions in different teams. This is the structure the experimental work identifies as the best carrier of complex contagion.

Its weakness is the mirror of the cluster's strength. The champions have no community, learn slowly, drift from the security function's intent, and are hard to reach quickly with an alert. Isolation also costs retention, which the champions literature repeatedly names as the main risk to the role.



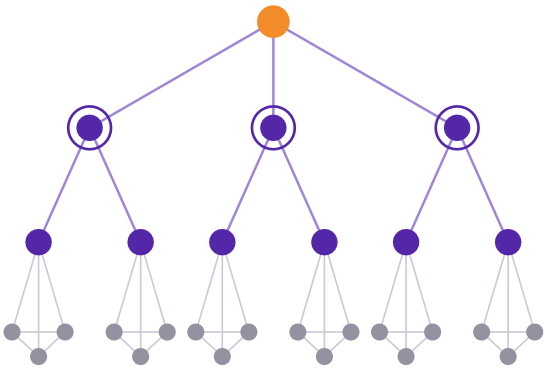
MODEL 4 · THE REFERENCE MODEL

Distributed champions with a thin backbone

Carries information via the backbone · Carries behaviour within teams · Across teams if the bridges are wide

Model 3 plus a sparse set of ties among champions and back to the security function. The backbone is thin on purpose: its job is to carry alerts, which need few ties, and identity, which needs even fewer. A handful of long ties between champions in different business units is enough to make the backbone a short-path network for information.

The design has to resist the pull towards Model 2, because the champions' community is pleasant and the team's resistance is not. In practice: fewer all-champion calls and more local work, a channel for broadcast rather than discussion, and recognition tied to what changed in the champion's team rather than to attendance.



MODEL 5

Tiered hierarchies

Depends on what the tiers are made of

Large organisations add tiers: lead champions in each division sit above local champions, and the security function talks to the leads. Tiers manage span of control rather than contagion, and can be laid over any of the first four models.

If the tiers are reporting lines, they add path length and a point of failure at each lead without adding reinforcement. If the leads are themselves embedded in their divisions and the tiers are used to build wide bridges between neighbouring teams, they can help behaviour cross department boundaries, which is where it most often stalls.

MODEL	PATHS FROM CENTRE	CLUSTERING AROUND COLLEAGUES	TIES AMONG CHAMPIONS	CARRIES INFORMATION	CARRIES BEHAVIOUR	MAIN RISK
Hub and spoke	Short	Low	None	Outward only	No	Single points of failure; nothing flows back
Single champion cluster	Short	Low	Dense	Yes, among champions	Among champions only	Network runs parallel to the business
Distributed, embedded	Long	High	Sparse or none	Slowly	Yes, within teams	Isolation, drift, slow alerts, attrition
Distributed with backbone	Short via backbone	High	Thin	Yes	Yes; across teams if bridges are wide	Backbone grows into a cluster
Tiered hierarchy	Depends on tiers	Depends on base model	Structured	Yes	Only if leads create wide bridges	Added path length and failure points

A single cluster, or a clustered network?

The words are close and the structures are opposites. In a **single cluster** the champions are clustered with each other. In a **clustered network** each champion is clustered with their own colleagues, and the champions as a group are only lightly connected.

The single cluster is the attractive mistake, and its attractions are all real. It builds capability, because champions learn from each other faster than from the security function. It builds retention, because belonging keeps people in a voluntary role. It is visible, so it is easy to report on and easy to fund. And it is where information moves best: a message dropped into the cluster reaches every champion within a day.

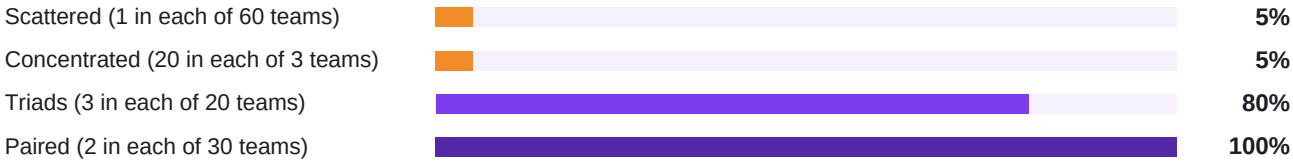
What it does not do is move behaviour in the teams. Closure, the pattern in which a person's contacts also know each other, is the structural basis for norms, because it lets a group observe, sanction and reward its members. A single cluster has high closure among the champions and none between a champion and their team. The norms that form in it are the champions' norms.

> *“I built this model without meaning to. The champions' own community was the most visible and most rewarding part of the programme, and I invested in it accordingly. It took me longer than it should have to see that the pattern of ties I had built ran parallel to the business rather than through it.”*
>
> Andy Wood, CyBehave founder

A clustered network puts the closure where the behaviour needs to change. Two or three champions in a team of twenty, who know each other and who each know most of the team, give every colleague several adopting contacts at once. Once a team has tipped, the team itself becomes the reinforcement for anyone who joins it later.

The same sixty champions, placed differently

Illustrative simulation: 1,200 employees, 60 teams of 20, 60 champions. Share of the organisation adopting a behaviour that needs three reinforcing contacts, after 120 periods, in clustered teams with long cross-team ties.



For an alert (one exposure is enough) all four placements reach the whole organisation within about fifteen periods. For the behaviour, no colleague of a scattered single ever sees three adopters, so nobody starts; the concentrated cluster saturates its three teams and stops at the boundary. Means of twenty runs.

How much reinforcement decides how much placement matters

The same runs with a lighter behaviour, where two adopting contacts are enough.

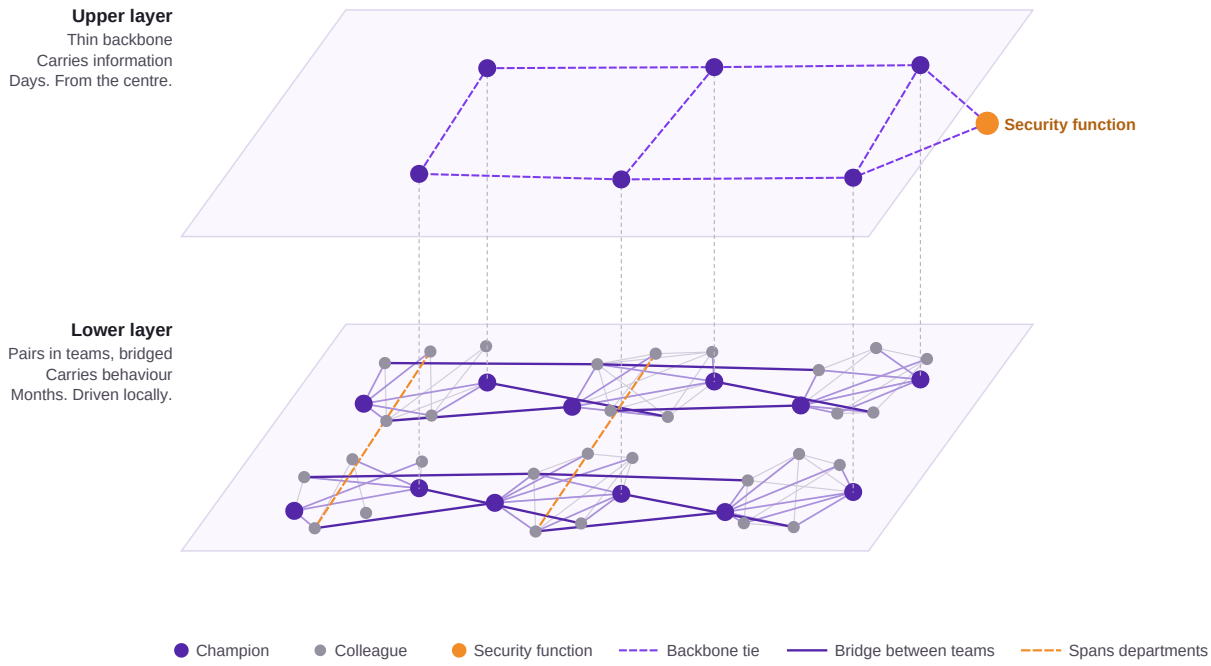


For a mildly complex behaviour, coverage is nearly enough. For one that needs real reinforcement, which includes most of the behaviours a security function cares about, coverage is beside the point and placement is everything. The simulation is an illustration of the mechanism, not evidence that it holds in a real organisation. The study that would settle it is a placement comparison in a live programme, with the behaviour measured directly.

Build in two layers, and keep them distinct.

A network that has to carry both kinds of contagion should be built as two layers, each shaped for what it carries. The **lower layer** places champions in pairs or triads inside the teams whose behaviour is the target, chosen by nomination for their position in the team, with wide bridges between neighbouring teams and some ties that span departments. This is where behaviour moves, in months, driven locally.

The **upper layer** is a thin, organisation-wide backbone among champions, with the security function attached to it rather than at the centre of it. This is where information moves, in days, driven from the centre. The backbone is held sparse so that it never becomes the champions' home. Seven parameters set the shape, and the contagion argument gives each one a direction the roster view does not.



The two layers, with each champion appearing on both. Six teams in two departments; two champions in each team, tied to each other and to most of the team; several ties between neighbouring teams and a couple that span departments; and above it all a sparse backbone that carries alerts and identity, with the security function attached at the edge rather than sitting at the centre.

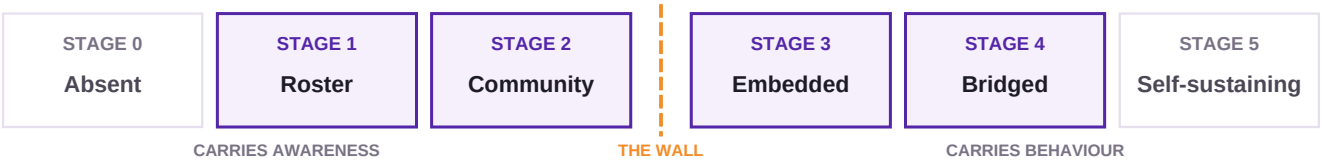
PARAMETER	THE ROSTER VIEW	THE CONTAGION VIEW
Champion ratio	One per 20 to 50 employees	Secondary; what matters is seeds per team
Local seed density	Not considered	Two or three champions per target team, tied to each other
Selection	Interest in security; volunteers	Position in the team; nomination by colleagues
Coverage	Every unit has a champion	Every target behaviour has a tipped team nearby
Ties among champions	As many as possible	Thin; a small-world backbone for alerts and identity
Bridge width	Not considered	Several ties between neighbouring teams; some spanning departments
Measure of success	Champions recruited, sessions held	Behaviour adopted by colleagues; exposure counts; teams tipped

Reading your own network

None of this needs more than a short survey, a spreadsheet and a network library. Ask each person who they go to for security advice, who they would tell about a suspicious message, and who they talk to about work, and six things can be read from the answers: **exposure count** (how many adopting contacts each non-adopter has, which is the direct measure of whether behaviour can start); **champion embedding** (the share of a champion's security ties that lie inside their own team, which a single cluster shows up as low); **modularity** against team membership; **bridge width** between neighbouring teams and between departments; **champion betweenness**, which finds the people who should carry the backbone and are often not the embedded ones; and the simple count of **tipped teams** and the teams next to them. What most programmes lack is not the tooling. It is the decision to measure reach rather than coverage.

The network models and the three journeys

The homepage routes you by where you are: Getting Started, Running Your Network, or Beyond Awareness. The network models matter at each point, in different ways, and they line up with the stages of the Security Champions Maturity Model.



Models 1 and 2 are the networks a programme builds at Stages 1 and 2, and they carry awareness. Models 3 and 4 are what Stages 3 and 4 require, and they carry behaviour. The wall between them is a change of shape. Read the maturity model

GETTING STARTED · STAGES 0 TO 1

Design the lower layer from day one

You will build a hub and spoke first, and that is fine: it is the easiest transition in the model and it gets alerts to every team. The mistake is to let the roster decide where champions go.

- Recruit in pairs per target team, not singles everywhere
- Ask teams who they go to, and recruit those people
- Decide now that you will count what reaches colleagues

cybehave.com/getting-started

RUNNING YOUR NETWORK · STAGES 1 TO 2

Recognise which model you have built

If your champions know each other better than they know their teams, you have Model 2. It will keep reporting success on coverage, attendance and content while the behaviour line stays flat.

- Measure champion embedding, not just activity
- Thin the community into a backbone
- Move attention from the champions to the teams

cybehave.com/running-your-network

BEYOND AWARENESS · STAGES 3 TO 5

Rebuild the shape, then widen the bridges

Behaviour change at scale is the two-layer reference model made real: pairs and triads in target teams, bridges between neighbouring teams and across departments, and a backbone held thin.

- Pair seeded teams with unseeded ones
- Place champions on existing cross-team ties
- Count exposure and tipped teams

cybehave.com/beyond-awareness

Measuring reach, not just coverage.

HEROES by CyBehave is built around the idea that the programme's view of itself is one vantage point and not enough. The core platform measures what reaches colleagues: the **Behaviour Index** comes from the quarterly Team Pulse, in which colleagues rate the security behaviours they observe in their own team, independent of the champions and of the training platform. The coverage map and the Champion influence map show which teams have a champion and how security actually spreads. The **Network Optimisation** module, in development, is where the measures on this page live: who bridges teams, who is isolated, whose position carries a message furthest, recruitment targeting drawn from the gaps, and succession risk where coverage rests on one person.

The working paper

The position on this page is set out in full, with the simulation, its limits and the references, in a working paper from the CyBehave Lab. The paper also describes the field study that would test the argument: an organisation with a champions programme, a network survey at two points a year apart, a behaviour measured directly, and champion placement varied between business units.

Wood, A. (2026). Network models for Security Champions: Design variations, contagion dynamics and the choice between a clustered network and a single cluster. Working paper, version 1, 24 October 2026. CC BY 4.0.

- Preprint to follow
- The companion paper: the maturity model
- Back to the Lab

Glossary

The terms from network and behavioural science used in this document, in plain English.

Adopter. Someone who has taken up the behaviour, or who knows the piece of information. In the simulations the champions start as adopters, and the question is how many of their colleagues become adopters too.

Backbone. A deliberately thin set of ties among champions, and back to the security team, kept for alerts and a sense of identity and nothing more.

Betweenness. How often a person sits on the shortest route between two others. People with high betweenness are the natural carriers of alerts across an organisation.

Bridge. The ties that join one team to another. Bridge width is how many there are. A single tie is a narrow bridge: fine for news, too narrow for behaviour, which needs several ties into the next team before it can cross.

Champion embedding. The share of a champion's security-related conversations that happen inside their own team rather than with other champions or the security team. Low embedding is the signature of a champion cluster.

Closure. The pattern in which your contacts also know each other, forming a closed loop. Closure lets a group notice, reward and gently correct behaviour, which is how norms form.

Clustering. How far a person's contacts also know each other. In a tightly clustered team everyone talks to everyone, so several people can show the same behaviour at once. A random network has almost no clustering.

Community of practice. A group of people who do the same kind of work and learn from each other through regular contact. Champion communities usually become one, and it does them good.

Complex contagion. Spread that needs reinforcement: a person takes up the behaviour only after seeing several people they know do it. Most security behaviours work this way, because they cost effort, feel risky, or break a habit.

Contagion. Borrowed from epidemiology: anything that spreads from person to person through contact, whether a piece of news, a habit or a norm. Nothing bad is implied by the word.

Exposure count. For each person who has not yet adopted a behaviour, the number of their contacts who have. It is the direct test of whether the behaviour can start to spread to them.

Long tie. A tie that reaches into a different team or group from your own. Long ties carry news quickly across an organisation. They carry behaviour badly, because the person at the far end sees only one example of it.

Modularity. A measure of how strongly a network splits into separate groups, such as teams, with many ties inside each group and few between them. High modularity means strong team clusters.

Path length. How many hops a message takes to get from one person to another through the network. Short paths mean fast spread of information.

Reinforcement. Seeing the same behaviour from more than one person you know, at the same time. One example is a curiosity; several at once make it the normal thing to do.

Seeding. Where you place the first adopters. Champions are the seeds. The same number of them, placed differently, produces very different spread.

Simple contagion. Spread that needs only one exposure. Hearing an alert or a rumour once is enough to pass it on. Information behaves this way, which is why it travels fast through any shape of network.

Tie. A working relationship between two people: they talk, ask each other for advice, or would pass on a warning. Network diagrams draw ties as lines. It is the pattern of ties, not the org chart, that decides what spreads.

Tipped team. A team in which most people now do the behaviour, so the team itself keeps it going and shows it to newcomers and to neighbouring teams.

About this document

This document was built on 24 November 2026 from the page at cybehave.com/champion-network-models, 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/champion-network-models

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. Written by Andy Wood, founder of CyBehave. You are welcome to share this document with colleagues. Please keep it whole and credit CyBehave.