ANDY WOOD

THE RISE OF THE SECURITY CHAMPION

From Awareness to Action

Contents

PREFACE: Why this book exists

Three years ago, I watched a manufacturing company's cybersecurity programme collapse overnight. Not because of a breach. Not because of budget cuts. But because the one person who held it all together left for another role.

Sarah Mitchell had built something remarkable at Meridian Manufacturing. She'd recruited 28 Security Champions, reduced phishing susceptibility by 58%, and won awards for her leadership. Her champions didn't just respect her professionally; they genuinely liked her and wanted to support her vision. When she left, the whole thing fell apart within six months.

The mistake wasn't that Sarah left. Talented people will always have opportunities. The mistake was that the organisation had built something dependent on one person's energy and relationships rather than creating sustainable infrastructure. They'd built a *programme*, not a *capability*.

I've spent over a decade working with organisations of all sizes to embed security into their business and their culture. I've seen brilliant programmes thrive and well-intentioned initiatives quietly fade away. I've watched small businesses achieve remarkable results with small budgets, and I've seen multinational corporations struggle

despite unlimited resources. The difference rarely comes down to money or technology. It comes down to understanding people.

This book exists because security is fundamentally a human challenge. You can deploy the most sophisticated tools available, write comprehensive policies, and mandate training for everyone in the organisation. But if people don't understand why security matters, if they don't feel equipped to make good decisions, if the culture doesn't support secure behaviour, your defences remain fragile.

Security Champions are how you change that equation. They're not replacing your security team. They're extending their reach into every corner of the organisation. They're the colleagues who help others understand that protecting information isn't someone else's job; it's part of everyone's job. They make security feel accessible rather than intimidating, practical rather than theoretical.

But here's what most organisations get wrong: they think Security Champions programmes are about security awareness. They're not. They're about behavioural change. That's why this book draws heavily on evidence from behavioural science, not just cybersecurity best practices. We need to understand why people behave insecurely before we can effectively help them behave more securely.

This isn't a theoretical exercise. Every framework, every recommendation, every case study in this book comes from practical experience. I've watched programmes scale successfully and seen others collapse under their own weight.

The good news? We now know what works. The patterns are clear. Organisations that follow certain principles create programmes that deliver sustainable value. Organisations that skip steps or ignore cultural realities struggle, regardless of how much they invest.

This book gives you those patterns. It shows you how to design a Security Champions programme that fits your organisation's context, how to secure the executive support you'll need, how to recruit and develop champions who want to be involved, and how to measure impact in ways that matter to your business. It also shows you what failure looks like and how to avoid it.

I've written this for everyone who's tired of being the lone voice talking about security. For the IT manager who knows there must be a better way to build secure digital practices. For the business leader who understands that security isn't just IT's problem. For anyone who recognises that their organisation's people could be its greatest defence rather than its weakest – especially in the digital era.

The journey ahead isn't easy. Building a Security Champions programme requires patience, persistence, and a willingness to

invest in people rather than just technology. But the organisations that make this investment don't just become more secure - they become more resilient, more aware, and better equipped to navigate whatever digital challenges emerge next.

Your organisation has people who care about doing good work. People who want to protect the business and their colleagues. People who would step up if they knew how.

Security Champions gives them that opportunity.

Let's begin.

PART I: FOUNDATIONS

Chapter 1: Why Security Champions Matter

The ransomware attack hit the hospital network at 3:47 on a Tuesday morning. By 7:00, when the security team arrived, the damage was catastrophic. Patient records were encrypted. Surgical systems were offline. The emergency department had reverted to paper records while ambulances were diverted to other hospitals.

The attack vector? An accounts payable clerk had clicked a link in an email that appeared to come from a trusted supplier. The email was sophisticated; it referenced a real invoice number and perfectly mimicked the supplier's branding. The clerk had no reason to suspect anything was wrong. She was just trying to do her job efficiently.

Here's the part that haunts the CISO: two weeks earlier, a different employee in the purchasing department had received a similar email. That employee found it suspicious, forwarded it to IT, and the security team updated their filters. But they never thought to tell accounts payable. They never created a way for that purchasing employee to share what she'd learned with her colleagues across the organisation.

If there had been a Security Champion in that department, someone who understood both the work of accounts payable and the nature of phishing attacks, someone who had relationships across the finance team and knew how to communicate security concerns without creating fear, that attack likely wouldn't have succeeded.

This is why Security Champions matter. Not because they're security experts. Not because they replace your security team. But because they're positioned exactly where security decisions happen - in the daily work of every department, every function, every level of your organisation.

The Limits of Traditional Security

For decades, we've approached cybersecurity the same way: centralise expertise, deploy technology, write policies, deliver awareness training, and hope for the best. This model worked reasonably well when organisations had clear perimeters, limited connections, and relatively stable threat landscapes.

That world no longer exists.

Today's organisations are borderless. Your employees work from home offices, coffee shops, and client sites. Your systems live in the cloud. Your data flows through dozens of third-party services. Your

people use personal devices for work and work devices for personal tasks. The traditional perimeter has dissolved.

Meanwhile, threats have become more sophisticated and targeted. Attackers don't just probe technical defences anymore; they study your organisation, understand your workflows, and craft attacks that exploit the gap between what policies say and how people work. They know that the most sophisticated firewall in the world can't protect you if someone authorises a wire transfer to a fraudulent account.

Your security team can't be everywhere. They can't review every email, every decision, every interaction. They can't understand the context of every business process across every department. They can't scale to meet the distributed nature of modern work.

This creates a dangerous gap. Security teams know what needs to happen, but can't be present where decisions are made. Employees make dozens of security-relevant decisions daily, but often lack the knowledge or confidence to make them well. Between those two realities, vulnerabilities emerge.

Security Champions bridge that gap.

What Security Champions Actually Do

A Security Champion is not a part-time security professional. They're not an additional job that gets piled onto someone's already full workload. They're an employee who continues to do their primary role but brings security awareness to how that work happens.

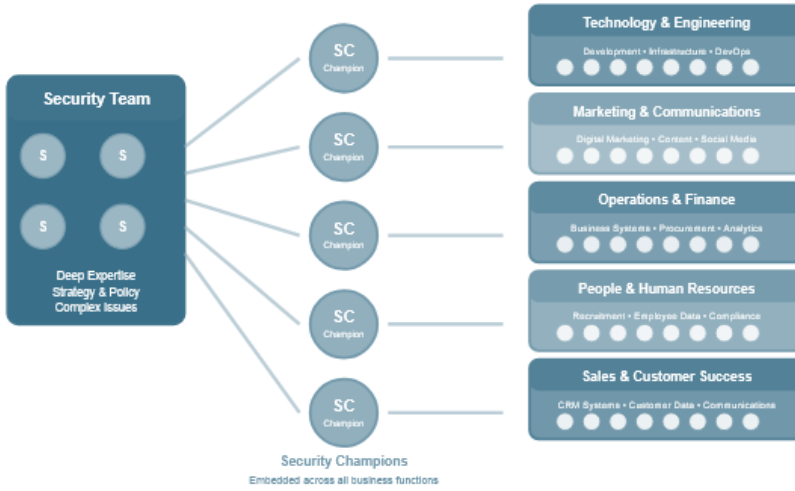

Figure 1 Champions bridge the gap: bringing security expertise to where decisions are made.

Think of them as translators. The security team speaks in technical language about vulnerabilities, patches, and threats. Business teams speak in terms of deadlines, customer needs, and operational efficiency. Champions translate between these worlds. They make

security relevant by connecting it to what people really care about in their day-to-day work.

A champion on your sales team understands why the sales process requires certain security controls and why the standard approval workflow doesn't work for urgent customer situations. They help the security team understand real-world constraints and help the sales team implement security without killing deals. They're the voice that says, "*Here's how we can protect customer data and still close business before quarter-end.*"

A champion in your development team advocates for security considerations during design, not just during the security review that happens three weeks before launch. They ask the questions that catch potential issues early: "*How are we handling authentication here?*" "*What happens if this API gets called with unexpected input?*" "*Should we log this action for audit purposes?*"

A champion on your HR team considers security implications when designing new processes. When HR moves to a new recruitment platform, the champion considers what applicant data is being collected, where it's stored, and who has access. They're not blocking progress; they're ensuring that progress happens securely.

Champions also serve as early warning systems. They're embedded in their teams, so they notice things that would never reach the

security team. They spot the workaround that everyone's using because the secure process is too cumbersome. They hear about the external consultant who's been given inappropriate access. They recognise when a new business process creates security risks that no one has thought about yet.

Perhaps most importantly, champions normalise security conversations. When security only comes from the central IT team, it feels like external oversight. When it comes from a trusted colleague, it becomes part of the work itself. Champions demonstrate through their own behaviour that thinking about security isn't paranoid or obstructionist; it's professional and responsible.

Why People Behave Insecurely

Before we go further, we need to address an uncomfortable truth: most security incidents aren't caused by malicious intent or gross negligence. They're caused by ordinary people doing ordinary work under ordinary pressures.

The accounts payable clerk who clicked that phishing link wasn't careless. She was experienced, conscientious, and followed established procedures. The email arrived during a busy period. It looked legitimate, and she had no reason to be suspicious. In that

moment, given what she knew and the context she was working in, clicking that link was the reasonable thing to do.

This is the fundamental challenge of security. We're not fighting against malicious insiders who want to cause harm. We're working with people who genuinely want to do good work but face dozens of competing demands. Security is rarely their primary objective. It's one consideration among many.

Think about your own behaviour. You know you should use unique passwords for every account. You probably don't. You know you should verify unexpected requests before acting on them. Sometimes you don't. Not because you don't care about security, but because in the moment, other priorities feel more urgent.

Understanding this reality is crucial for Security Champions. Their job isn't to police their colleagues or catch people doing things wrong. It's to make secure behaviour easier and more intuitive than insecure behaviour. It's to build understanding so people can make better decisions. It's to create an environment where asking "*Is this secure?*" feels as natural as asking *"Is this accurate?*"

We'll explore the behavioural science behind this in greater depth in the next chapter, but here's the key insight: people don't behave insecurely because they lack awareness. They behave insecurely

because the secure option is often harder, slower, or less clear than the insecure option. Security Champions help change that equation.

The Business Case for Champions

Let's be direct: Security Champions programmes require investment. Champions need time to participate, training to be effective, and ongoing support to stay engaged. You'll need to allocate budget, dedicate programme management resources, and secure executive commitment. That investment needs to deliver measurable value.

Here's what the evidence shows: organisations with mature Security Champions programmes report significant improvements across multiple dimensions.

Incident rates decline because problems get caught earlier and are prevented more often. When you have champions embedded across the organisation, more people are better able to recognise and report potential security issues sooner. The phishing email that might have compromised a department gets spotted and reported instead. The misconfigured system gets flagged before it goes into production. The risky workaround gets addressed before it becomes standard practice.

Project delivery accelerates because security isn't an afterthought that requires painful remediation late in the process. When you have

a champion involved in project planning from the start, security considerations get built in rather than bolted on. This prevents the costly security reviews that discover fundamental design problems weeks before launch. Teams still deliver quickly, but they deliver securely from the beginning.

The Hidden Cost of Late-Stage Security

A financial services company discovered during the final security review that its new customer portal stored passwords in reversible encryption rather than proper hashing. Fixing this required three weeks of additional development and a month-long delay in launch, resulting in approximately £200,000 in lost revenue and development time. A Security Champion involved in the initial design phase could have caught this on day one at virtually no cost.

Compliance becomes more consistent because you have eyes throughout the organisation who understand requirements and can spot gaps. Instead of relying solely on annual audits to discover compliance issues, champions help their teams maintain compliance continuously. When regulations change, champions help translate new requirements into practical changes in their teams' workflows.

Cultural shifts occur that extend far beyond specific security behaviours. Organisations with strong Security Champions programmes report improvements in cross-functional collaboration, increased employee empowerment, and a greater sense of shared ownership for organisational success. Champions don't just improve security culture; they often catalyse broader improvements in how the organisation works.

The return on investment is compelling. A typical Security Champions programme costs roughly 0.5 to 2 per cent of an organisation's IT security budget (depending on size and scope) but can reduce security incidents by 40 to 60 per cent and prevent costly delays in major projects. The avoided costs of a single prevented breach often exceed the entire annual programme investment.

But here's what's harder to quantify and potentially more valuable: resilience. Organisations with mature champion programmes are better equipped to adapt to new threats, technologies, and ways of working. They've built security capability throughout the organisation rather than concentrating it in a single team. When change happens, and it always does, they're positioned to respond effectively.

What This Book Will Show You

Building a Security Champions programme isn't simple, but it's not mysterious either. Organisations succeed by following certain patterns and fail by making predictable mistakes. This book gives you both: the patterns that lead to success and the mistakes that lead to struggle.

We'll start with foundations. The next chapter explores the behavioural science that makes Security Champions effective. You'll learn why traditional awareness training often fails and why peer influence succeeds. You'll understand the psychological factors that drive security behaviour and how to design programmes that work with human nature rather than against it.

Then we'll turn to execution. You'll learn how to build the business case that secures executive support, how to maintain that support through challenges, and how to handle the inevitable objections. You'll discover how to identify potential champions, recruit them effectively, and design a programme structure that fits your organisation's context. We'll cover training approaches that create genuine capability rather than just checking boxes, recognition strategies that sustain engagement, and measurement frameworks that demonstrate value.

We'll also examine what happens when things go wrong. You'll meet organisations whose programmes collapsed and learn from their mistakes. You'll see how successful programmes navigate common challenges. You'll gain practical wisdom about what really matters versus what sounds good in theory but doesn't work in practice.

Throughout, we'll ground everything in real examples. The five detailed case studies in Chapter 8 show you what success looks like in different contexts: a multinational IT company that scaled to 300+ champions, a charity that transformed security on a £5,000 budget, a bank that discovered the limits of mandated participation, a manufacturer that rebuilt after collapse, and a healthcare provider that proved that slow and steady wins the race.

Who This Book Is For

I've written this book for several audiences, all of whom play critical roles in making Security Champions programmes succeed.

If you're a Chief Information Security Officer or security leader, this book shows you how to extend your team's reach and impact without expanding headcount. You'll learn how to build the business case, secure resources, and measure outcomes in ways that demonstrate strategic value.

If you're an IT manager or director who owns security as part of broader responsibilities, this book offers a pragmatic approach to building security capability without requiring deep security expertise. You'll find practical guidance on starting small, proving value, and scaling effectively.

If you're a business leader who recognises that security isn't just IT's problem, this book helps you understand how to make security everyone's responsibility in practice, not just in policy. You'll see how champions can become catalysts for broader cultural change beyond just security.

If you're a security professional who's tired of being the sole voice advocating for security, this book shows you how to create allies throughout the organisation who can amplify your message and extend your impact.

If you've been asked to start or run a Security Champions programme, this book is your implementation guide. It answers the practical questions that keep you awake at night: How do I recruit champions who really want to participate? How do I keep them engaged six months in? How do I prove this is working? What do I do when challenges arise?

The Journey Ahead

Building a Security Champions programme is a journey, not a destination. It requires patience, persistence, and willingness to adapt. You'll make mistakes. You'll face challenges you didn't anticipate. Not everything will work on the first attempt.

But organisations that commit to this journey transform their approach to security. They build resilience that extends far beyond mere attack prevention. They create cultures in which security is integrated into how work happens rather than being an external constraint imposed by IT. They develop people who feel empowered to protect the organisation rather than being told they're the weakest link.

Your organisation has people who care about doing good work. People who want to protect your business and your customers. People who would step up if they knew how and felt supported. Security Champions gives them that opportunity.

The chapters ahead show you how to make that happen. Let's begin building something sustainable.

Chapter 2: The Behavioural Science Behind Champions

Here's a story that will sound familiar. A large organisation invests heavily in security awareness training. Everyone completes the mandatory eLearning modules. People pass the quizzes, and completion rates reach 100 per cent. The training team celebrates success.

Three months later, phishing click rates have barely changed. People still write passwords on sticky notes. The same risky behaviours continue. The training delivered awareness but didn't change behaviour. Awareness, it turns out, is not the same as action.

This is why understanding behavioural science matters for Security Champions programmes. We're not trying to make people aware that security is important. Most people already know that. We're trying to help them behave more securely in the moment when it matters, under pressure, when they're busy and distracted and just trying to get their work done.

Security Champions work because they're designed around how people change behaviour, not how we wish they would. This chapter explains why.

The Awareness Trap

Let's start with why traditional security awareness programmes so often fail to deliver lasting change, despite good intentions and significant investment.

Most security awareness training operates on a simple assumption: if people understand the risks and know what they should do, they'll do it. Tell people that weak passwords are dangerous, and they'll create strong ones. Explain phishing techniques so they can spot malicious emails. Show them the consequences of a data breach, and they'll handle information more carefully.

This assumption is wrong. Not slightly wrong, but fundamentally wrong. Understanding what you should do is neither necessary nor sufficient for actually doing it.

Think about your own life. You know you should exercise regularly, eat more vegetables, save more money, and get more sleep. You probably know exactly what you should do in each case. But does that knowledge mean you always do it? Of course not. Knowing what

to do and actually doing it are different challenges that require different solutions.

The same applies to security behaviour. People who click on phishing emails usually know they should be careful about unexpected messages. They're not lacking awareness. They lack the *capability* to recognise sophisticated phishing in real time, the time to carefully scrutinise every email when managing 200 messages a day, or an organisational culture that values responding quickly over responding cautiously.

This is where behavioural science becomes valuable. It helps us understand the real barriers to secure behaviour, so we can design effective interventions.

Understanding Why People Behave the Way They Do

Figure 2 Capability, Opportunity & Motivation collectively deliver behavioural change

Behavioural scientists use various frameworks to understand human behaviour, but one of the most useful for security is the COM-B model. The name comes from three factors that must be present for any behaviour to occur: **C**apability, **O**pportunity, and **M**otivation.

Capability means having the *physical* and *psychological* ability to perform a behaviour. Physical capability might include having the right tools or resources. Psychological capability includes having the knowledge, skills, memory, and attention needed.

For security, capability issues appear everywhere. An employee might lack the knowledge to recognise a sophisticated social engineering attempt. They might not know how to use the approved file-sharing system. They might not have the cognitive resources to carefully evaluate every email when they're managing multiple urgent priorities simultaneously.

Opportunity means having the right context for the behaviour to happen. This includes both physical opportunity (the time, resources, and environmental factors) and social opportunity (the cultural norms and social cues from others).

Security behaviours often fail because of opportunity barriers. The secure file-sharing system might be so slow that people default to email attachments to meet deadlines. The process for reporting security concerns might require filling out a form that takes 15 minutes. The team culture might subtly punish people who slow things down by raising security questions.

Motivation includes both reflective processes (our conscious intentions and beliefs) and automatic processes (our habits, emotional responses, and impulses).

Most security training focuses exclusively on reflective motivation: trying to convince people they should care about security. But automatic motivation often matters more. If clicking 'Yes' on prompts

has become a habit, people will continue doing it even if they know they should read them carefully. If security feels like it conflicts with getting work done, people will choose productivity over security in the moment, regardless of what they believe in principle.

Here's the crucial insight: **all three factors must be present for behaviour to occur consistently**. If anyone is missing or insufficient, the behaviour won't happen reliably, no matter how strong the other factors are.

You can make people highly motivated to use strong passwords, but if they lack the capability to create and remember complex passwords across dozens of accounts, they'll fall back to reusing simple ones. You can give people both capability and motivation to report suspicious emails, but if the reporting process is cumbersome and they're not given time to do it, they won't report consistently.

This is why Security Champions are effective. They address all three factors simultaneously in ways that centralised security teams cannot.

How Security Champions Address the Behavioural Challenge

Champions build **capability** by making security knowledge accessible and contextual. Instead of generic phishing training, a

champion in your finance department can explain what invoice fraud looks like in your organisation's context, using real examples that feel relevant rather than abstract. They can demonstrate how to use security tools in ways that fit with actual workflows. They answer questions when people are uncertain rather than requiring people to seek out the security team.

This contextual knowledge is more effective than generalised awareness because it directly addresses the capability barriers people face. When your sales team champion explains how to share customer data securely without delaying deals, they're building capability in the specific moment and context where it's needed.

Champions create **opportunity** by identifying and addressing environmental barriers that prevent secure behaviour. Because they work within their teams, they see the practical obstacles that centralised security teams miss. They notice when the approved process is so cumbersome that everyone has developed workarounds. They recognise when security requirements conflict with operational realities. They can advocate for solutions that are both secure and practical.

Equally important, champions shape social opportunity by normalising conversations about security. When security questions come only from the IT department, they feel like external oversight. When they come from a trusted colleague, they become part of how

the team works. Champions demonstrate, through their own behaviour, that considering security is normal professional practice, not paranoia or obstructionism.

Champions strengthen **motivation** through both reflective and automatic processes. They help colleagues understand why security matters in terms that resonate with their work rather than in abstract terms. A champion in customer service can connect security practices to protecting customer trust in concrete terms. A champion in product development can frame security as quality and reliability rather than a compliance burden.

But champions also work on automatic motivation by helping establish security habits and routines. They can suggest simple practices that become automatic over time: always locking your screen when stepping away, consistently using a password manager, and routinely checking the sender address on unexpected emails. They reinforce these behaviours through regular interaction and peer modelling.

Why Peer Influence Works

Research consistently shows that peer behaviour influences our own behaviour more powerfully than expert instruction. We look to people like us to determine what's normal and acceptable. When a respected colleague models security-conscious behaviour, it affects our own behaviour more than a policy document or training module ever could. This is why champions embedded in teams are more effective than centralised security communications.

The Power of Social Proof

Humans are fundamentally social creatures. We constantly look to others to determine how we should behave, often unconsciously. This tendency, called social proof, is one of the most powerful forces shaping our behaviour.

When you're unsure how to act in a situation, you look at what others around you are doing. When you see most people behaving a certain way, that behaviour feels normal and appropriate. When you see behaviour that seems deviant or unusual, you're less likely to adopt it yourself.

Security teams have traditionally worked against social proof rather than with it. Security policies say "*You must do X*," but people observe that their colleagues rarely do X and never face consequences for

not doing X. The policy says one thing, but social proof says another. Guess which one wins?

Security Champions harness social proof positively. When a champion in your team consistently models secure behaviour, carefully scrutinising unexpected emails, using the password manager, or locking their screen, that behaviour becomes socially normal. Others begin adopting it not because they're following policy but because it's what people like them do.

This is particularly powerful when champions are well respected within their teams. If the person everyone trusts for advice, the one who's seen as competent and sensible, treats security as part of professional practice, others naturally follow. It's not about authority or compliance. It's about social norms.

Champions also make visible the secure behaviours that often happen invisibly. When someone carefully verifies an unusual request before processing it, that cautious behaviour is usually invisible to others. But when a champion tells *that* story, "*I received this urgent request that seemed odd, so I called to verify it, and it turned out to be fraudulent*", that careful behaviour becomes visible and socially reinforced.

The message shifts from "*You should be careful*" (a policy requirement) to "*Being careful is what we do here*" (a social norm). That shift is behaviourally powerful.

How New Behaviours Spread

Understanding how innovations spread through populations helps explain both why Security Champions work and how to design your programme for maximum impact.

Sociologist Everett Rogers developed a model showing that new behaviours or technologies spread through five groups: innovators adopt first (roughly 2.5% of the population), followed by early adopters (13.5%), then the early majority (34%), late majority (34%), and finally laggards (16%). Each group has different characteristics and responds to different influences.

When you launch a Security Champions programme, you're not trying to change everyone's behaviour simultaneously. You're trying to create *momentum* that carries through these different groups.

Your initial champions are likely to be your innovators and early adopters: people who are naturally interested in security, who enjoy being at the forefront of change, and who are motivated to be part of something new. These people are valuable for getting started, but they're not sufficient for achieving widespread change.

The crucial moment comes when you reach the early majority. These are pragmatists who adopt new behaviours not because they're novel but because they're proven and useful. They're influenced heavily by peer recommendations and visible evidence of value. This is where your programme either achieves mainstream adoption or stalls.

Security Champions help cross this chasm precisely because they provide peer recommendations and visible evidence. When the early majority see their colleagues succeeding as champions, hear directly from peers how it's helped them, and observe the benefits in their own teams, they're far more likely to adopt security-conscious behaviours themselves.

This is why scaling your programme thoughtfully matters more than scaling quickly. You need time for early champions to demonstrate value, for their peers to observe benefits, and for word of mouth to

Starting with Willing Volunteers

When recruiting your first champions, prioritise people who genuinely want to participate over achieving geographic or departmental coverage. Your innovators and early adopters will build momentum that makes it easier to recruit the early majority later. Forced participation at the start often backfires by creating visible examples of people who are unenthusiastic or resentful, which undermines social proof.

build credibility. Programmes that rush to universal coverage before building this foundation often struggle to achieve genuine adoption.

Making the Secure Choice the Easy Choice

Another key insight from behavioural science involves choice architecture: how the way options are presented affects which option people choose. Small changes in how choices are structured can have dramatic impacts on behaviour, often without people being consciously aware of the influence.

Consider a simple example. If you want people to use a password manager, you could mandate it through policy. That requires motivation and often generates resistance. Alternatively, you could make it the default option that's already installed and configured, with an explanation of how to use it. People can still choose not to use it, but the path of least resistance now leads to the secure behaviour.

This principle, sometimes called nudging, involves designing environments so that the easiest or most intuitive option is also the secure option. It works with human nature rather than against it.

Security Champions are excellent at identifying where nudges could be valuable because they work within real workflows. They see where friction exists, where people develop workarounds, where the secure

option requires extra effort that people under time pressure won't consistently make.

They can advocate for changes that make security easier: suggesting that the approved file-sharing system be integrated directly into email rather than requiring a separate website visit, proposing that security requirements be built into templates, so people don't have to remember to add them, and recommending that sensitive data classification happen automatically based on content rather than requiring manual tagging.

Champions can also design lightweight nudges within their own teams. Simple interventions, such as placing hand sanitiser at obvious locations, significantly increase handwashing rates. Similarly, placing prominent reminders at key decision points can increase secure behaviour: a visual reminder near the door prompting people to lock their screens when leaving, a checklist integrated into the project kick-off template that includes security considerations, and a quick reference card near the phone showing how to verify unusual requests.

These nudges work because they address opportunity barriers and reduce the cognitive effort required for secure behaviour. They don't rely on people maintaining constant vigilance or making explicit decisions every time. They make security the path of least resistance.

Building Security Habits

Much of our daily behaviour happens automatically through habits rather than conscious decision-making. This is efficient; imagine having to consciously think through every routine action. But it means that changing behaviour often requires changing habits, not just changing intentions.

Habits form through repetition in consistent contexts. When you perform a behaviour repeatedly in response to the same cue, your brain creates an automatic association. Eventually, the cue triggers the behaviour without conscious thought. This is why you automatically buckle your seatbelt when getting in a car or automatically lock your front door when leaving home.

Security behaviours can become habitual in the same way, but only if they're repeated consistently in stable contexts. This is difficult when security behaviours are sporadic (for example, responding to phishing emails occurs occasionally rather than daily) or when contexts vary (for example, what constitutes suspicious changes between routine supplier emails and unexpected executive requests).

Security Champions help build habits in several ways. They can establish simple routines that become automatic through repetition, such as locking your screen whenever you step away. Using the

password manager for every login becomes automatic when you do it repeatedly. Checking sender addresses becomes automatic when you do it routinely.

Champions also help by making security behaviours more consistent and predictable. When there's a clear, simple procedure for handling potentially sensitive information - always use the secure portal, no exceptions - people can develop habits. When the procedure varies depending on circumstances and requires judgment, habits can't form as easily.

More importantly, champions can help establish social habits within teams. If your team has a routine of reviewing security considerations at every project kickoff, that becomes a team habit that persists even when specific team members change. If your department shares suspicious emails in a Slack channel for others to learn from, it creates a learning habit that reinforces individual awareness.

The key to habit formation is making the behaviour simple, repeatable, and consistently cued. Champions are positioned to help their teams establish these conditions in ways that centralised security teams cannot.

Why Traditional Approaches Often Fail

Understanding these behavioural principles helps explain why so many well-intentioned security initiatives fail to deliver lasting change.

Annual compliance training fails because it focuses solely on building awareness (which is insufficient) and does so in a context completely separated from where behaviour actually occurs. People might learn something during the training, but without the opportunity to practice immediately in their real work context, and without environmental support for the new behaviour, little change. The annual cadence also means any learning has faded long before the next training opportunity.

Fear-based messaging about the consequences of security failures attempts to increase motivation through anxiety. Research shows this approach often backfires. Moderate fear can motivate action if people feel capable of responding effectively. But high fear without clear, achievable actions leads people to disengage entirely. "If the threats are that sophisticated and the consequences that severe, there's nothing I can do anyway, so why worry about it?" Fear without capability building is counterproductive.

Technical controls alone address capability and opportunity only in limited ways, but they ignore motivation and often create new

barriers to opportunity. Requiring complex passwords increases security but decreases usability, leading to password reuse across accounts (making them less secure overall). Blocking certain websites might prevent some risky behaviour, but it can also create frustration that motivates people to find workarounds. Technical controls are necessary but insufficient.

Policies and mandates attempt to motivate through compliance requirements but do nothing to address capability or opportunity barriers. Mandating behaviour that people lack the capability to perform consistently or the environmental support to maintain simply creates a gap between policy and practice. People learn to appear compliant during audits, whilst reverting to familiar behaviours the rest of the time.

The Knowing-Doing Gap

Research across many domains shows that information rarely changes behaviour on its own. Doctors knowing what treatment is best doesn't ensure they prescribe it. People knowing they should exercise doesn't ensure they do. Security is no different. Closing the knowing-doing gap requires addressing capability, opportunity, and motivation simultaneously, which is exactly what effective Security Champions do.

Creating Identity-Based Change

One final behavioural principle deserves attention: the power of identity. People are motivated not just by what they want to achieve but by who they want to be. When behaviour connects to identity, how we see ourselves and how we want others to see us, it becomes more sustainable and self-reinforcing.

Traditional security messaging often positions employees as the problem: "*You're the weakest link*." This creates a negative identity association. Security becomes something imposed on people who can't be trusted rather than something people do because it's part of professional competence.

Security Champions programmes can create positive identity associations instead. Being a champion means being someone who helps colleagues, who has valued expertise, who contributes to organisational success. Champions aren't being monitored for compliance; they're being recognised for contribution.

This identity shift can extend beyond champions themselves. When champions successfully embed security into team culture, team members begin to see themselves as people who take security seriously. It becomes part of professional identity: *"We're the team that protects customer data*," not "*We're the team that has to follow security rules*."

This identity-based motivation is powerful because it's intrinsic rather than extrinsic. People behave securely not because they're monitored or incentivised but because it's consistent with who they are and how they see themselves. This type of motivation sustains through challenges and persists even when external oversight is absent.

Champions facilitate this identity shift through language and framing. Instead of talking about security as compliance burden, they frame it as professional competence. Instead of positioning security as IT's job that others must accommodate, they position it as shared responsibility that everyone contributes to. These seemingly small framing differences have meaningful behavioural impacts over time.

Pulling It All Together

Let's return to where we started: why Security Champions work when so many other approaches to security awareness fail.

Champions work because they address behaviour change comprehensively rather than superficially. They build capability through contextual education and support. They create opportunity by removing barriers and establishing supportive environments. They strengthen motivation through both rational and emotional

pathways. They harness social proof, facilitate habit formation, improve choice architecture, and enable identity-based change.

None of this requires champions to be behavioural science experts. These principles operate whether or not people consciously apply them. But understanding these principles helps you design Security Champions programmes more effectively.

When you recruit champions, you're not just selecting people with security knowledge. You're identifying people who can influence peer behaviour, who are positioned to observe and address opportunity barriers, who can help establish team habits and norms.

When you train champions, you're not just teaching security concepts. You're building capability to translate security into context-specific guidance, to recognise behavioural barriers, to facilitate conversations that shift team culture.

When you measure impact, you're not just tracking incident rates. You're looking for evidence of capability development, opportunity improvements, motivation strengthening, and behaviour change across your organisation.

The chapters ahead show you how to apply these principles practically. You'll learn how to design programme structures that support behaviour change, how to recruit and develop champions

who can facilitate it, how to measure whether it's actually happening, and how to sustain it over time.

But everything builds on this foundation: Security Champions work because they're designed around how people actually change behaviour, not around how we wish they would change behaviour. They work with human nature rather than against it. And that's why they succeed where so many other approaches fail.

Applying Behavioural Science

Doesn't Require Expertise

*You don't need a degree in psychology to apply these principles. Simply asking three questions consistently will help: What **capability** does this behaviour require? What **opportunity** barriers might prevent it? What would **motivate** someone to do this? If any factor is weak, strengthen it before expecting behaviour change. This simple framework will guide better decisions throughout your programme design.*

PART II: BUILDING YOUR PROGRAMME

Chapter 3: Securing Executive Sponsorship

You can design the most elegant Security Champions programme in the world. You can have perfect training materials, brilliant recruitment strategies, and innovative engagement approaches. None of it matters if you don't have executive sponsorship.

Not approval. Not permission. Not a polite nod in a meeting followed by "*sounds interesting, keep me posted*." Real sponsorship. The kind where executives actively protect the programme when priorities shift, where they ask about progress in leadership meetings, where they personally recognise champions, and where they intervene when department heads push back.

Here's the uncomfortable truth that took me years to accept: executives don't care about Security Champions programmes. They care about business outcomes, risk reduction, operational efficiency, regulatory compliance, and competitive advantage. Your job isn't to make them care about Security Champions. Your job is to show them how Security Champions delivers what they already care about.

This chapter shows you how to do that. How to build a business case that resonates with executive priorities, how to pitch it effectively, how to handle inevitable objections, and how to maintain executive engagement once you've secured it. Think of it as learning to speak executive as a second language.

Why Executive Sponsorship Actually Matters

Before we discuss how to secure executive support, let's be clear about why it's not optional.

Executives control three things your programme cannot succeed without: budget, time, and organisational priority.

Budget might seem obvious, but it's not just about initial funding. It's about protecting resources when cost pressures emerge. Every organisation faces periodic budget reviews, restructures, and "*do more with less*" mandates. Programmes without executive champions get quietly defunded during these exercises. Programmes with executive sponsorship get protected because someone with authority says, "*This stays.*"

Your Security Champions programme needs funding for training, recognition, tools, and programme management. These costs aren't enormous, but they're real. Without executive protection, they're vulnerable every budget cycle.

Time is actually more critical than money. Champions need time to participate in training, attend meetings, support colleagues, and contribute to security initiatives. That time comes from somewhere, which means it's not being spent on other work. Managers are judged on their team's delivery. Unless those managers receive clear signals from above that champion participation is valued and expected, they'll deprioritise it whenever deadlines loom.

I've watched programme after programme struggle because champions get pulled back to *real work* during busy periods. The message is clear: security culture matters until something else matters more. Executive sponsorship is what makes champion time non-negotiable rather than optional.

Organisational priority shapes what people actually pay attention to amid competing demands. Every employee faces dozens of priorities. Projects, deadlines, customer issues, internal initiatives, and improvement programmes all compete for mind share. People take cues from leadership about what really matters versus what's just nice to have.

When executives visibly support Security Champions by attending events, recognising contributors, asking about progress, and discussing it in leadership communications, the organisation pays attention. When executives are silent or absent, everyone assumes it's not really that important. This isn't cynical; it's realistic. People

have learned through experience that executive attention reliably predicts organisational priority.

Consider what happens when challenges emerge. Every programme faces them: engagement dips, department heads complain about time commitments, competing initiatives launch, and organisational changes create uncertainty. Without executive sponsorship, these everyday challenges become programme-threatening crises. With it, they're manageable obstacles that get addressed.

Here's a concrete example. A sales director complains that their champion is spending too much time on *security stuff* and not enough on customer relationships. Without executive backing, you're negotiating from a position of weakness. You're asking the sales director to prioritise something that doesn't appear in their objectives or compensation. You'll lose.

With executive sponsorship, the conversation is different. The sales director receives a message from their boss or their boss's boss: "*Security Champions is a strategic priority. Let's discuss how we support both sales targets and security objectives*." That's not a negotiation; it's a directive. The conversation shifts from whether the champion participates to how to make participation work alongside other responsibilities.

This executive air cover is invaluable. It protects your programme and your champions from being gradually squeezed out by day-to-day operational pressures.

Understanding the Executive Perspective

Securing executive support requires understanding how executives think about priorities, risks, and investments. They operate in a different world than security professionals, facing different pressures and evaluating decisions through different frameworks.

Executives balance competing demands constantly. They're accountable for business performance, shareholder value, regulatory compliance, customer satisfaction, employee engagement, and operational efficiency, all simultaneously. New initiatives are evaluated not in isolation but against every other possible use of finite resources. Your Security Champions programme competes for attention with product launches, market expansion, digital transformation, cost reduction, and countless other priorities.

This competition is fierce. Most executive teams receive more proposals for new initiatives than they could possibly support. The default answer to any new proposal is "*no*" or "*not now*" simply

because resources and attention are limited. Understanding this context shapes how you approach executive sponsorship.

Executives think in terms of outcomes, not activities. They don't get excited about training programmes, awareness campaigns, or cultural initiatives. They care about results. When you say "*Security Champions programme*," they hear "*another thing that will consume resources*." When you say "*reducing security incidents by 40 per cent while accelerating project delivery*," you're speaking their language.

Risk is another lens executives use constantly, but they think about risk differently than security professionals. Security teams think about technical vulnerabilities, threat actors, and attack vectors. Executives think about business impact, reputation damage, regulatory exposure, and strategic risk. The translation matters.

Instead of "*we have insufficient security awareness creating vulnerability to social engineering attacks*," say "*we're vulnerable to data breaches that could cost us £500,000 in direct response plus regulatory fines plus customer trust damage*." Same risk, different framing. One is technical; the other is business impact.

Executives also evaluate every initiative through the lens of return on investment, whether the return is formally calculated or intuitively assessed. They're constantly asking: "*Will investing these resources*

here deliver more value than investing them somewhere else?" Your job is to make that case clearly and credibly.

The Language Gap

Security professionals and executives often speak different languages about the same things. Security says, "Reduce attack surface." Executives hear "technical jargon." Security says, "improve security posture." Executives hear "vague objective." Security says, "prevent security incidents that would cost £500,000, delay projects by an average of three weeks, and risk regulatory penalties." Executives hear "measurable value." Learn to translate.

This doesn't require elaborate financial models. It requires showing that the investment (champion time, training costs, programme management) is substantially smaller than the avoided costs (security incidents, project delays, compliance failures, productivity losses). Make the math simple and the logic clear.

Finally, executives want initiatives that support organisational strategy, not distract from it. If your organisation is focused on digital transformation, position Security Champions as enabling secure digital transformation. If customer trust is strategic, frame it as protecting customer relationships. If operational efficiency matters, emphasise how champions prevent costly security delays. Never position Security Champions as separate from strategy. Position it as supporting the execution of the strategy.

Building Your Business Case

Now let's construct the business case that will resonate with executive priorities. This isn't about what you want to build; it's about what problems you'll solve and what value you'll create.

Start with the problem, not the solution. Executives need to understand why this matters before they care about what you're proposing. Don't open with "*I want to establish a Security Champions programme*." Open with the business problems that Security Champions will solve.

What's the current state? Are security incidents causing operational disruption? Are security reviews delaying projects? Are you receiving compliance findings from regulators? Do employees feel unsupported on security matters? Are you seeing risky workarounds because official processes are too cumbersome?

Quantify wherever possible. "*Security delays added an average of 23 days to our last five major projects*" is more compelling than "*security sometimes slows projects down*." "*We had eight reportable security incidents last year, averaging £180,000 in direct response costs*", beats "*incidents happen occasionally*."

If you don't have hard data, gather it. Interview project managers about security-related delays. Review incident reports for common

root causes. Survey staff about their security confidence. This homework dramatically increases credibility. Executives trust evidence more than assertions.

Once you've established the problem, connect it explicitly to what your organisation cares about strategically. If digital transformation is a priority, explain how security friction impedes digital adoption. If customer trust matters, link security incidents to a decline in customer confidence. If operational efficiency is a focus, show how security issues waste time and money.

Look at your organisation's strategic plan, annual report, or executive communications. What language do they use? What goals do they emphasise? Echo that language in your business case. You're not manipulating; you're translating. You're helping executives see how Security Champions supports objectives they're already committed to achieving.

Now introduce Security Champions as the solution. Explain the model concisely: a distributed network of peer influencers embedding security awareness into day-to-day operations. Why this approach rather than alternatives? Because centralised security teams can't scale to meet distributed needs. Because peers influence behaviour more effectively than policies. Because embedding security into workflows is more effective than separating it.

Describe what success looks like. Be specific and concrete: champions in every major business unit, security considerations integrated into planning discussions, staff feeling confident handling security decisions, measurably reduced incidents and delays, improved compliance metrics, stronger organisational culture. Paint the picture of the future state. Make it tangible.

Provide evidence that this works. Executives trust proof more than promises. Reference specific examples from other organisations, being careful to protect confidentiality where needed. Cite research on peer influence and security culture. If you've run a pilot, present those results prominently.

This evidence serves two purposes. It demonstrates that you've done your homework and aren't proposing something untested. It also gives executives confidence that success is achievable rather than aspirational.

Be transparent about what you're asking for. Executives value honesty about costs more than they value lowball estimates that later require additional funding. Break down the investment clearly:

Champion time commitment, typically two to four hours monthly per champion. Training and development costs for initial and ongoing education. Programme management resources to coordinate, support, and measure the programme. Tools and platforms needed

for communication and collaboration. Recognition and engagement activities to maintain motivation.

Frame this as an investment, not a cost. You're investing in organisational capability that will deliver returns over time. Show the math.

Now demonstrate the expected return. This is where many business cases fall apart. They detail costs but leave benefits vague. Be specific about what will improve and by how much.

Reduced security incidents mean fewer direct response costs and less operational disruption. Faster project delivery from shorter security review cycles. Improved compliance means fewer regulatory findings and lower audit costs. Enhanced staff productivity from less time dealing with security issues and more confidence in decisions.

Use conservative estimates. If you think you can reduce incidents by 50 per cent, estimate 30 per cent. If you can reduce project delays by 15 days, estimate 10. Credibility matters more than optimism. Under-promise and over-deliver is a better strategy than over-promise and under-deliver.

Translate improvements into financial terms where possible. If reducing project delays by 10 days saves £50,000 per project, and

you have 12 major projects annually, that's £600,000 in value created. If preventing one major security incident saves £400,000 in response costs and business disruption, and you prevent two incidents annually, that's £800,000 in avoided costs.

The investment in Security Champions is typically a fraction of these returns.

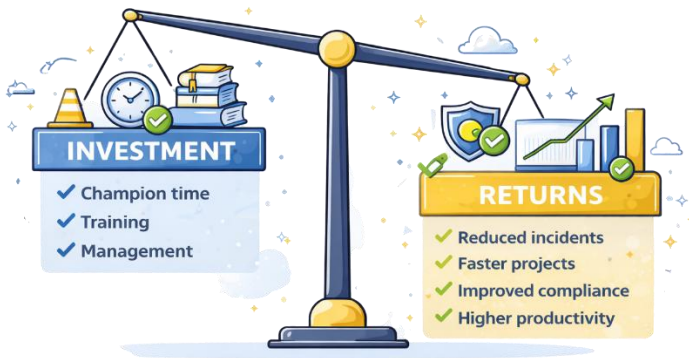

Figure 3 The return on a security champion programme outweighs the investment.

Address implementation pragmatically. Executives want to know this is realistic, not just theoretical. Outline the implementation approach: how you'll recruit champions, what the timeline looks like, how you'll measure progress, what risks you've anticipated and how you'll mitigate them.

Big-bang launches often fail. Propose a phased approach: pilot in two or three business units, demonstrate value, then expand based

on lessons learned. This reduces initial investment, enables early results, and allows course correction. It also signals that you're pragmatic and risk-aware, qualities executives value.

Consider offering tiered options: a minimum viable programme, a recommended programme, and an enhanced programme. Different resource levels, different scopes, different timelines. This gives executives agency in the decision. They're not just approving or rejecting; they're choosing the right level of investment for your organisation's context.

Pitching to Leadership Effectively

You've built a solid business case. Now you need to deliver it in a way that lands with your specific audience.

Know your audience. Who are you pitching to? The CISO? The COO? The full executive committee? Each audience has different priorities and different contexts.

The CISO already understands security value; you're selling implementation approach and business alignment. The CFO cares about costs, returns, and financial risk. The COO focuses on operational efficiency and productivity. The CEO thinks strategically about organisational capability and competitive positioning.

Tailor your pitch to your audience without changing the fundamentals. Emphasise what matters most to them whilst covering all essential elements.

Start with the problem, not your solution. Don't open with "*I want to talk about Security Champions.*" Open with "*I want to talk about how we can reduce the security-related project delays costing us 23 days per project and protect customer trust more effectively*."

You've got their attention because you're addressing problems they already know exist. Security Champions comes in as the solution, not as the starting point.

Use their language. Pay attention to how executives talk about the business. Do they use military metaphors? Business school language? Operational terms? Mirror their language naturally. This isn't about being inauthentic; it's about communicating in ways that resonate.

Keep it concise. Executives are time-poor. Your pitch should be deliverable in 10 to 15 minutes, with additional detail available if needed. Prepare a one-page executive summary, a short slide presentation (five to 10 slides maximum), and supporting documentation for them to review later.

Get to the point quickly. Problem, solution, evidence, investment, return, approach. Don't bury your message in excessive detail. You can always provide more information in response to questions.

Make it concrete with stories. Numbers matter, but stories stick. Share a brief anecdote about a security incident that could have been prevented by a champion spotting the issue early. Describe a champion from another organisation who helped their team integrate security into a major project smoothly.

Stories make abstract concepts concrete. They help executives visualise what you're proposing. When someone asks a question six months from now about what Security Champions actually do, they'll remember your story more readily than your bullet points.

Address concerns proactively. Anticipate questions and objections, then address them in your pitch before they're asked. Common concerns include:

Won't this be extra work for already-busy employees? No, because we're recruiting genuinely interested people, providing meaningful recognition, and integrating into existing work rather than adding separate activities.

Will this actually change culture, or is it just more awareness theatre? Case studies show measurable impact on behaviour and outcomes,

not just awareness scores. We're designing for behaviour change using evidence-based approaches.

How do we know champions won't lose interest after initial enthusiasm? That's why we're investing in ongoing engagement, community building, and demonstrating continuous value rather than treating this as a launch-and-forget initiative.

What if department heads don't support releasing people for champion activities? That's why we need executive sponsorship to signal this is a priority and to protect the champion's time from competing demands.

Proactively addressing concerns demonstrates you've thought critically about implementation challenges. It builds confidence that you're realistic about difficulties rather than naive about them.

Be specific about what you need. Don't end with "so, what do you think?" End with specific requests:

Approval for a six-month pilot in three business units with this specific budget. An executive sponsor who will attend quarterly champion events and address obstacles. Agreement to protect champion time from competing demands. Commitment to review pilot results and make a scale-up decision.

Clarity about what you need makes it easier for executives to say yes. Vague requests generate vague responses.

Securing Genuine Sponsorship

Getting approval is step one. Getting genuine ongoing sponsorship requires more deliberate effort.

Identify the right sponsor. The best executive sponsor is someone who has sufficient authority to protect the programme and allocate resources, understands or is willing to learn about the value of security culture, has credibility across the organisation, and is willing to be actively involved, not just provide passive endorsement.

Often, this is the CISO, COO, or CIO. Sometimes it's a forward-thinking business unit leader. Don't default to the most senior person

Practice Your Pitch

Rehearse with colleagues who can play the role of sceptical executives. Have them challenge your assumptions, question your numbers, and raise objections. Prepare detailed answers for likely questions about costs, timelines, measurement, risks, and alternatives considered. If you don't know an answer, say so honestly and commit to finding out. Credibility matters more than having every answer immediately.

available. Find the person who will be genuinely engaged.

Define expectations explicitly. Once you've identified your sponsor, have a frank conversation about what active sponsorship looks like. You might request attendance at quarterly champion events, willingness to intervene when department heads deprioritise champion activities, participation in programme communications such as endorsement emails and recognition announcements, and quarterly reviews of progress and challenges.

Make the ask concrete so your sponsor knows what they're committing to. Vague sponsorship becomes passive support. Specific expectations enable active engagement.

Communicate regularly. Don't only reach out when you need something or when there's a problem. Establish regular touchpoints. Perhaps monthly 15-minute check-ins or quarterly deeper reviews. Use these touchpoints to share progress, celebrate wins, raise emerging challenges, and seek guidance.

This keeps your sponsor informed and engaged. It prevents the common pattern in which sponsors only hear about programmes when something goes wrong.

Make sponsorship easy. Provide your sponsor with ready-made content they can use with minimal effort. Brief updates they can

share in executive meetings. Recognition announcements can be sent with minor editing. Talking points for when they're discussing the programme with peers.

The easier you make it for your sponsor to be visibly supportive, the more likely they are to do it consistently. Most executives want to support good initiatives but are time-constrained. Remove friction wherever possible.

Deliver early wins. Nothing sustains executive sponsorship like evidence of value. Prioritise achieving and communicating early successes. A department that reduced security delays. A champion who detected a potential incident early. Positive feedback from business stakeholders. Any tangible evidence that the programme is delivering value.

Share these wins with your sponsor promptly and make it easy for them to share upward and outward. Early success builds executive confidence that their sponsorship is well-placed.

Handling Common Objections

Even strong business cases face pushback. Here's how to address the objections you're most likely to encounter.

"We don't have a budget for this."

Response: The investment is quite modest, primarily champion time that we're leveraging from existing resources. The training and programme management costs are significantly less than the costs we're currently bearing from security incidents and delays. We're asking to redirect existing resources more effectively, not add substantial new costs.

Consider showing the cost breakdown. If incidents cost you £300,000 annually and project delays cost £400,000, and your programme costs £50,000, the math is compelling.

Also offer: "*Would a smaller pilot help? We could start with two business units and demonstrate value before scaling. The pilot investment would be roughly £15,000 over six months*."

"People are already too busy. They won't have time for this."

Response: That's precisely why we need Security Champions. Currently, security issues create unplanned work through incidents, delays, and rework. Champions help prevent these issues, ultimately saving time. We're also recruiting people who are genuinely interested, not mandating participation across the board.

We estimate two to four hours per champion per month. That's less time than it takes to resolve a typical security incident, and we'll

prevent multiple incidents. The time investment prevents larger time losses.

"Can't the security team just handle this?"

Response: The security team is handling what centralised security can address: tools, policies, and infrastructure. But security teams can't scale to embed security awareness into every team's daily operations. That requires distributed champions who understand local context and have peer influence.

This isn't replacing the security team's work; it's extending their reach through multipliers across the organisation. It's like the difference between having one teacher for 500 students versus having one teacher plus 20 teaching assistants who work with smaller groups.

"How do we know this will actually work?"

Response: This is why we're proposing a pilot approach. Let's test in these specific business units for six months and measure results. We'll track security incidents, project delays, staff confidence, and engagement levels. If it works, we scale. If it doesn't, we've limited our exposure.

Also, reference evidence: "*Similar organisations have demonstrated measurable results. [Cite specific example.] We're not experimenting blindly; we're applying proven approaches adapted to our context.*"

"What if people participate initially but engagement fades?"

Response: That's a real risk, which is why we're building engagement mechanisms from the start: community building, ongoing training, meaningful recognition, visible impact. We'll monitor engagement metrics monthly and intervene early if we see a decline.

The case studies show that programmes with proper investment in champion experience sustain engagement. The ones that fade are those that treat champions as unpaid labour without support.

"This sounds like a nice-to-have, not a must-have."

Response: Let's look at the business impact of our current state. [Present specific costs of incidents, delays, and compliance issues.] These are real costs we're bearing now. Security Champions addresses root causes rather than just symptoms.

Frame it in terms of risk: "*We can invest £50,000 in prevention or continue spending £300,000 annually managing consequences. Which represents better stewardship of resources?*"

The Objection Behind the Objection

Sometimes the stated objection isn't the real concern. "We don't have a budget" might really mean "I'm not convinced this is a priority." "People are too busy" might mean "I don't want to deal with pushback from department heads." Listen for the underlying concern and address that rather than just the surface objection.

Maintaining Executive Engagement

Securing initial executive support is important. Maintaining it over time is essential. Here's how to keep your sponsor engaged as the programme matures.

Deliver on commitments. Nothing erodes executive confidence faster than missing promised milestones or failing to deliver expected outcomes. Be realistic in your initial commitments, then meet or exceed them. Under-promise and over-deliver creates confidence. Over-promise and under-deliver destroys it.

If challenges emerge that will prevent you from meeting commitments, raise them early with your sponsor and propose solutions. Executives can handle problems if they're warned early and presented with options. They can't handle being surprised at the last minute.

Communicate wins visibly. When champions achieve something noteworthy, share it promptly with your sponsor in a format they can easily pass along. "*Our champion in operations spotted a phishing campaign targeting our supply chain and alerted IT before anyone clicked. Estimated prevention value: £200,000*."

Make it easy for your sponsor to look good by supporting the programme. Give them stories they can tell in leadership meetings about tangible value being delivered.

Measure what matters to them. Track metrics that resonate with executive priorities, not just security metrics. Yes, measure incident rates and compliance scores. But also measure project delivery times, employee confidence scores, and cost avoidance.

Present metrics in business terms. Don't just say *"phishing click rate decreased from 18 per cent to 6 per cent*." Say *"phishing click rate reduction prevented an estimated three incidents that would have cost £150,000 each to remediate."*

Seek their input regularly. Treat your sponsor as an advisor, not just a resource. Ask their perspective on challenges you're facing. Seek their guidance on strategic decisions. This creates engagement and investment. People support what they help create.

It also gives you access to an executive perspective that can help you navigate organisational dynamics and align with broader priorities.

Adapt to changing context. Organisations change constantly. New priorities emerge. Leadership turns over. Market conditions shift. Security Champions programmes that succeed in the long term are those that adapt to a changing context whilst maintaining their core purpose.

Stay attuned to shifts in organisational focus and proactively adjust how you position and operate the programme. If the organisation suddenly focuses on cost reduction, emphasise cost avoidance and efficiency. If growth becomes the priority, emphasise enabling secure scaling.

Your sponsor can help you navigate these shifts if you keep them informed and seek their counsel.

Prepare for sponsor transition. Eventually, your sponsor will move roles, leave the organisation, or shift focus. Plan for this inevitability. Document the sponsorship relationship. Build relationships with other potential sponsors. Ensure the programme has support beyond any single individual.

When the transition happens, brief the new sponsor thoroughly. Don't assume they understand the programme's history, value, or needs. Give them reasons to continue supporting it. Make it easy for them to maintain momentum rather than starting from scratch.

The Sponsorship You Need

Let me be direct about what effective sponsorship looks like in practice, because it's easy to mistake passive approval for active support.

Effective sponsors attend champion events, not every time, but regularly enough that champions recognise their engagement. They don't just send someone from their office; they show up personally, speak briefly about why it matters, and stay to interact with champions.

Effective sponsors intervene when obstacles arise. When a department head complains about champion time commitments, the sponsor has a conversation about priorities. When budget pressures threaten programme resources, the sponsor protects them. When champions need access to senior stakeholders, the sponsor facilitates it.

Effective sponsors communicate about the programme beyond just approving it. They mention it in leadership meetings. They recognise

champions in company communications. They ask about progress in one-on-ones with their direct reports. They signal consistently that this matters.

Effective sponsors challenge the programme constructively. They ask hard questions about impact and value. They push for evidence and measurable results. This isn't unsupportive; it's engaged. It makes the programme better and ensures it continues to deliver value that warrants their continued support.

Passive sponsors approve the programme but then fade into the background. They're too busy to attend events. They don't respond when obstacles emerge. They never mention it in broader communications. The programme technically has executive support but not executive sponsorship. The difference matters enormously for long-term success.

If you find yourself with passive rather than active sponsorship, you have two options. Either work to convert passive into active by making engagement easier and demonstrating clear value, or find a different sponsor who will be genuinely engaged. A programme with no official sponsor but genuine grassroots support often fares better than one with an official sponsor who's disengaged.

Making the Ask

We've covered why executive sponsorship matters, how to build the business case, how to pitch effectively, and how to maintain engagement. Let's close with practical guidance on actually making the ask.

Schedule dedicated time. Don't try to secure executive support in a brief hallway conversation or at the end of a meeting about something else. Request a specific meeting for this purpose. Give executives time to prepare and give yourself time to present properly.

Send materials in advance. Provide your executive summary and supporting documents before the meeting. Some executives will read them thoroughly; others won't look until the meeting. Either way, you've given them the option to come prepared.

Bring the right people. If you're pitching to multiple executives, consider who should join you. Someone from the business who can speak to operational benefits? An existing champion who can share personal experience? Sometimes you're more effective alone. Sometimes a small team is better. Choose strategically.

Be prepared for immediate questions or delayed decisions. Some executives will make decisions in the meeting. Others will want time

to think or consult with colleagues. Both are normal. If they defer the decision, ask about the process and timeline so you know what to expect.

Follow up promptly. After the meeting, send a brief summary of the discussion, any commitments made, and next steps. This creates a written record and ensures everyone has the same understanding of what was decided.

If you receive approval, move quickly to deliver early wins. Nothing validates executive confidence like seeing results soon after approval.

If you don't receive approval, ask for specific feedback about what would need to change for reconsideration. Sometimes "*no*" means "*not now*." Sometimes it means "*not like this*." Understanding the specific concern helps you decide whether to revise and resubmit or focus elsewhere.

Don't be discouraged by initial rejection. Many successful programmes were initially declined, revised based on feedback, and approved on the second or third attempt. Persistence, combined with responsiveness to feedback, often succeeds where immediate approval doesn't come.

The Foundation for Everything Else

Executive sponsorship isn't just about getting permission to start a programme. It's about building the foundation that enables everything else in this book to succeed.

Without executive sponsorship, recruiting champions is difficult because you can't protect their time. Training is limited because you lack a budget. Recognition is constrained because you have no authority to make it meaningful. Measurement is frustrating because you can't secure the data or resources needed. Scaling is impossible because you don't have organisational support.

With executive sponsorship, all these things become manageable. Not easy, but achievable. You have resources to invest, authority to make asks, protection from competing pressures, and credibility with stakeholders.

The effort you invest in securing and maintaining executive sponsorship pays dividends throughout your programme's lifecycle. It's the single most important factor determining whether your Security Champions programme will thrive or quietly fade away when challenges emerge.

So before you rush into programme design, recruitment, or training, invest time in securing genuine executive sponsorship. Build the business case thoroughly. Pitch it effectively. Convert passive

approval into active engagement. Maintain that engagement deliberately.

Everything else builds on this foundation. Get this right, and you've dramatically increased your chances of long-term success. Get this wrong, and even the best programme design will struggle to survive.

Now that you understand why executive sponsorship matters and how to secure it, we're ready to explore what you'll actually build: the design of your Security Champions programme itself.

Chapter 4: Designing Your Champions Network

Most Security Champions programmes fail not because they lack executive support or security expertise, but because they're designed for an idealised organisation that doesn't exist. The programme looks perfect on paper: clear roles, comprehensive training, elegant governance structures. Then it collides with reality.

Reality includes teams that already feel overstretched, managers who don't understand why security needs dedicated champions, technical stacks that vary wildly across the organisation, and cultures that resist anything resembling additional process. Your programme succeeds when it's designed for your organisation's actual context, not for the context you wish existed.

This chapter walks through the design of a champions network that works in practice. We'll explore how to assess your organisational context, structure your network appropriately, recruit champions who'll actually engage, and build sustainable operational models. The goal isn't the most sophisticated programme but the most effective one for your reality.

Assessing Your Organisational Context

Before designing anything, you need to understand the environment in which your programme will operate. Organisations differ dramatically in their structures, cultures, technical landscapes, and security maturity. A champions network that thrives in a flat, engineering-led startup will struggle in a hierarchical financial services firm with rigid compliance requirements.

Understanding Your Structure

Start with the basics. How is your organisation actually structured? Not what the organisational chart shows, but how work actually gets done, and decisions actually get made.

Some organisations operate through clearly defined teams with stable membership and well-understood responsibilities. Others have fluid team structures where people move between projects constantly. Some have strong functional hierarchies where security decisions flow through architecture boards and technical leadership. Others have autonomous product teams that make their own technical decisions with minimal central oversight.

These structural differences profoundly affect how champion networks function.

Sarah runs a champions programme at a large financial services firm. She described learning this lesson: "*We designed our programme based on the official org chart. Product-aligned champions who would embed security in their teams. Looked great in the slide deck. Completely ignored that most security-critical work happened in shared platform teams that served multiple products. We redesigned around actual work streams rather than official structures. Suddenly, champions were positioned where security decisions were actually made.*"

Map where security-relevant decisions happen in your organisation. Who decides which libraries to use? Who approves architectural changes? Who determines what security controls to implement? Your champions need to be positioned to influence these decisions, which means understanding where they actually occur rather than where they should occur in theory.

The Org Chart Trap

Formal organisational structures rarely reflect how work really flows. A technology company discovered this when their champions programme initially aligned with product divisions shown on the org chart. In practice, most security-critical decisions were made by the platform engineering team, which served all products. They had one champion covering dozens of crucial decisions, whilst product teams had multiple champions with limited security impact. Only after mapping actual decision flows did they realise their champion coverage was inverted.

Evaluating Your Culture

Organisational culture shapes what's possible more than most programme leaders acknowledge. Some cultures embrace volunteer-driven improvement initiatives. Others are deeply sceptical of anything not explicitly mandated by leadership.

You can't change your culture quickly, so your programme needs to work within it. This doesn't mean accepting every cultural limitation as unchangeable, but it does mean designing your initial approach to align with existing cultural norms whilst gradually shifting those norms over time.

Consider how your organisation typically adopts new practices. Does change happen through grassroots experimentation that later gets formalised? Or through top-down mandates that cascade through management layers? Does your organisation celebrate people who volunteer for additional responsibilities? Or does it operate strictly within defined role boundaries?

If your culture values volunteer contributions and grassroots innovation, you can build a champions network based on intrinsic motivation and distributed authority. If your culture is more hierarchical and process-driven, you'll need stronger executive sponsorship, more formal role definitions, and a clearer connection between champion activities and performance expectations.

Marcus leads a champions programme at a pharmaceutical company with a strong compliance culture. His approach reflects that context: "*We couldn't just ask people to volunteer as champions and figure it out as they went along. Everything needed formal definitions: role descriptions, manager approval, documented responsibilities, and clear escalation procedures. It felt bureaucratic compared to programmes at tech companies, but it worked for our culture. Champions had clarity and legitimacy because the programme operated within established norms.*"

Analysing Your Technical Landscape

The technical diversity in your organisation affects programme design more than most leaders anticipate. If your entire organisation uses three programming languages and two cloud platforms, you can build focused technical expertise in your champions. If you have twenty languages, five cloud providers, legacy on-premise infrastructure, and several generations of technology stacks, your challenges multiply.

Technical diversity isn't inherently bad, but it requires different programme design. You can't train all champions to an expert level across all technologies. You need to segment expertise, match champions to appropriate contexts, or develop different champion roles for different technical domains.

Map your technical landscape honestly. What languages do teams use? What platforms? What security tools? What development practices? Where are the consistencies and where are the variations?

Emma runs champions in a technology company that grew through acquisitions. Each acquired company brought different tech stacks and practices: "*We initially tried to create one standard champion training covering all our technologies. Impossible. A champion working in our legacy Java monolith faced completely different challenges than one working in our new Go microservices. We redesigned around technology domains. Champions received foundational training in security principles, then domain-specific training for their actual tech stack. Much more effective*."

Cultural Signals to Watch

How does your organisation respond when someone volunteers for additional work? If they're celebrated and supported, volunteer champions will thrive. If they're viewed suspiciously or asked why they're not focused on their "real" job, you'll need more formal mandate. How are cross-functional initiatives typically received? If people embrace them as opportunities, your champions network can operate fluidly. If people view them as distractions, you'll need stronger executive backing and clearer business justification.

Gauging Security Maturity

Your organisation's current security maturity determines your programme's starting point and realistic scope. A mature security organisation with established practices, knowledgeable engineers, and a strong security culture needs different champion support than an organisation just beginning its security journey.

Use a simple maturity assessment focused on practical realities rather than compliance frameworks. Do developers understand common security vulnerabilities in your tech stack? Do teams include security considerations in their design discussions? Are there established processes for security reviews and threat modelling? Do people know who to ask when they have security questions?

If your security maturity is low, your champions programme might initially focus on basic security literacy and establishing fundamental practices. As maturity increases, champions can work on more sophisticated challenges such as security architecture, advanced threat analysis, or security automation.

Importantly, maturity often varies significantly within organisations. Your newest product team might have strong security practices because they hired experienced engineers. Your legacy platform team might struggle with security basics because they've been

focused on keeping ageing systems running. Don't assume uniform maturity across your organisation.

Figure 4 Types of Champions Programme based on technical diversity and security maturity

Structuring Your Network

Once you understand your context, you can design a network structure that fits. The right structure depends on your organisation's size, complexity, distribution, and how work gets done.

Coverage Models

The most fundamental question is how to achieve appropriate champion coverage across your organisation. Different models work for different contexts.

Team-based coverage assigns champions to specific teams or departments. Each team has a designated champion responsible for security within that team. This works well in organisations with stable team structures and clear boundaries. The champion becomes the point person for security for everything their team does.

This model creates clear ownership and accountability. Everyone knows who their champion is. But it requires enough champions to cover all relevant teams, which may be challenging in large organisations or those with high technical diversity, where each team needs domain-specific expertise.

Domain-based coverage assigns champions to technical domains or security specialisms rather than teams. You might have champions focused on application security, cloud security, identity and access management, or data protection. Teams engage with the champion whose domain matches their current needs.

This model works well when you have high technical diversity or when security work crosses team boundaries. Champions develop deep expertise in their domains. But coordination becomes more complex because teams interact with multiple champions rather than having a single point of contact.

Hybrid models combine approaches. You might have team-based champions for routine security matters with domain specialists

available for complex issues. Or regional champions who provide general coverage with technical specialists for specific challenges.

Rachel runs a programme at a mid-sized technology company: *"We tried pure team coverage first. Didn't work because our teams were too small and specialised. A champion in our mobile team couldn't help the backend teams, and vice versa. We shifted to domain coverage, with champions specialising in frontend, backend, infrastructure, and API security. Teams now reach out to the relevant domain champion based on their work. Much better expertise matching."*

Network Size and Density

How many champions do you need? There's no universal answer, but you can calculate a reasonable range based on your organisation's

Start Simple, Evolve Later

Don't try to implement the perfect coverage model from day one. Begin with a simple structure that makes sense for your context, then evolve based on what you learn. It's easier to adjust coverage models after you understand how champions and teams interact than to design the optimal structure in theory before launching. Your first model should be good enough to start, not perfect enough to finish.

characteristics.

Consider champion-to-staff ratios. A common starting point is one champion per 30-50 staff in technical roles. If you have 300 engineers, that suggests 6-10 champions. But this ratio varies based on your context.

Higher security risk or regulatory requirements may need denser coverage. Financial services or healthcare organisations often target ratios of 1:20 or 1:30. Lower-risk environments might perform well with 1:50 or 1:75.

Technical complexity affects required density. If teams use diverse technologies requiring specialised security knowledge, you need more champions to cover the range of expertise. If technology is relatively uniform, fewer champions with broader coverage may suffice.

Security maturity influences how much support each champion needs. In low-maturity organisations, champions require more intensive support from the security team, which limits how many champions the security team can effectively enable. As maturity increases, champions operate more independently, allowing the same security team to support more champions.

Don't try to achieve full coverage immediately. Start with partial coverage in high-priority areas, prove value, then expand. A small network of effective, well-supported champions delivers more value than a large network of overwhelmed, under-supported champions.

The Coverage Trap

An insurance company launched with ambitious coverage targets: every technology team would have a champion within three months. They recruited 47 champions simultaneously. The security team couldn't provide adequate training or support. Champions felt abandoned and unclear about expectations. Within six months, 31 of the 47 had quietly disengaged. The programme nearly collapsed. They rebuilt with just 12 champions, provided intensive support, demonstrated value, and then gradually expanded to 35 highly engaged champions over the next year. Slower start, stronger finish.

Geographic and Temporal Distribution

If your organisation spans multiple locations or time zones, the network structure needs to account for distribution. Champions in different regions face different challenges, including varying local regulations, cultural norms around security, language barriers, and limited opportunities for face-to-face collaboration.

Consider whether you need regional coordinators who understand local context and can adapt programme elements appropriately

whilst maintaining overall consistency. These coordinators bridge between central programme leadership and regional champions.

Time zone differences affect how champions collaborate and access support. If your champions span Asia, Europe, and the Americas, you can't rely solely on synchronous meetings. You need asynchronous communication patterns, regionally scheduled events, and support models that work across time zones.

Virtual-first organisations require different approaches than co-located ones. You can't depend on hallway conversations and in-person workshops. Everything must work remotely, which changes how you build community, deliver training, and maintain engagement.

James runs a programme across a global technology company: *"We have regional leads in each major geography who coordinate local champions and run regional events. We have a mix of global and regional meetings. Global sessions are recorded and time-friendly for at least two regions, with the third region watching the recordings. Regional sessions are held at times convenient for local participants. We over-invest in written communication and documentation because we can't rely on everyone being in the same conversation simultaneously."*

Recruiting Champions Who'll Actually Engage

The success of your programme depends entirely on the people you recruit as champions. Recruit the wrong people, and no amount of structure or support will create an effective network. Recruit the right people, and even an imperfect programme can thrive.

Understanding Motivation

Why would someone volunteer to be a security champion? Understanding genuine motivations helps you recruit people who'll stay engaged rather than those who drop out after initial enthusiasm fades.

Some people are intrinsically interested in security. They find security challenges intellectually engaging, they're curious about how systems can be attacked and defended, and they enjoy the problem-solving aspects. These champions often stay engaged because the work itself is rewarding.

Others see champions as a development opportunity. They want to build security expertise that makes them more valuable professionally. They're motivated by learning, by gaining skills their peers don't have, by positioning themselves for career advancement. These champions engage when they see clear development outcomes.

Some are motivated by organisational visibility. Being a champion gives them exposure to leadership, involvement in strategic discussions, and recognition beyond their immediate team. They value the profile and connections that come with the role.

Others are motivated by team impact. They've seen their team struggle with security issues, they want to help their colleagues avoid problems, they care about their team's success and see champions as a way to contribute. These champions are often highly effective within their teams but may be less interested in broader programme activities.

No single motivation is superior. Effective programmes have champions with different motivations. But understanding what drives individual champions helps you provide appropriate support and recognition.

Ask Why They're Interested

During recruitment conversations, explicitly ask why someone wants to be a champion. Listen carefully to their answer. If they struggle to articulate clear motivation beyond "it seems like I should" or "my manager suggested it," that's a warning sign. Champions who don't have genuine reasons to engage often don't maintain engagement. Those with clear, personal motivations are much more likely to sustain commitment.

Identifying Champion Characteristics

What makes someone likely to be an effective champion? While individuals vary, certain characteristics predict success.

Technical credibility within their context. Champions don't need to be the most senior or most experienced engineers, but they do need sufficient technical knowledge for their peers to take them seriously. A champion who doesn't understand how their team's systems work can't provide useful security guidance.

This doesn't mean requiring security expertise initially. Many excellent champions began with minimal security knowledge but strong technical foundations. What matters is being technically capable enough to learn security concepts and apply them to real systems.

Communication capability. Champions need to explain security concerns in ways their teams understand, ask productive questions in design discussions, and advocate for security without alienating colleagues. Technical brilliance without communication skills limits champion effectiveness.

Look for people who already translate complex technical concepts for non-technical stakeholders, who help onboard new team members, and who can navigate disagreements constructively. These communication patterns transfer well to champion roles.

Demonstrated initiative. Effective champions see problems and address them without waiting for explicit direction. They're comfortable operating with some ambiguity; they take ownership of issues even when those issues aren't strictly their responsibility. Passive individuals who wait to be told exactly what to do struggle in champion roles.

This doesn't mean requiring aggressive personalities. Many quiet, thoughtful individuals show initiative in how they approach problems and follow through on commitments. The key is self-direction, not volume.

Time availability. Realistically, championing requires time. Someone who's already overwhelmed with their primary responsibilities can't take on champion duties effectively. Look for people who have capacity or can create capacity, not those already stretched thin.

This often means avoiding the most senior engineers who are juggling multiple high-priority commitments. Mid-level engineers with solid technical skills and manageable workloads often make excellent champions because they have time to engage meaningfully.

The "Best Engineer" Mistake

A software company initially recruited only its most senior, highest-performing engineers as champions. Made sense on paper: these people had the most expertise and the most influence. In practice, most dropped out within six months. They were already overcommitted. They didn't have time for champion training or community engagement. They saw champion work as a distraction from their core responsibilities. The second cohort recruited a mix of mid-level and senior engineers, explicitly screening for available capacity. Much higher sustained engagement because these champions invested the necessary time.

Balancing Volunteers and Nominations

Should you rely on volunteers who express interest in being champions, or should you nominate specific individuals you want to recruit? The best approach often combines both.

Open recruitment invites anyone interested to apply. This surfaces people with genuine motivation who might not otherwise be considered. It signals that the programme values volunteers rather than conscripts. But it may miss strong potential champions who don't self-nominate.

Targeted recruitment identifies specific individuals who'd be excellent champions and personally invites them. This ensures you

recruit people with the right characteristics, even if they haven't volunteered. But it may recruit people out of obligation rather than genuine interest.

A hybrid approach works well: open a recruitment period for volunteers whilst also approaching specific individuals with personal invitations. Some of your best champions will come from each path.

Katie runs a champions programme at a financial services firm: "*We do both. We send out open calls for volunteers and provide clear descriptions of what's involved. We also have team leads nominate people they think would be excellent champions, and we reach out to those people personally. About 60% of our active champions came through direct recruitment, and 40% through volunteers. The volunteers often bring more initial enthusiasm. The recruited ones often bring more sustained capability. We need both.*"

The Selection Conversation

Whether someone volunteers or gets nominated, have a proper conversation before confirming them as a champion. This isn't an interview to exclude people but a mutual exploration of fit and expectations.

Explain clearly what being a champion involves: time commitment, responsibilities, support available, and expectations. Be honest about

both challenges and opportunities. Someone who joins with unrealistic expectations will become frustrated and disengage.

Understand their motivation and what they hope to gain. Confirm that their reasons for being interested align with what the programme can offer. If someone wants deep security specialisation but your programme focuses on generalist engagement, address that disconnect.

Discuss practical constraints. Do they have manager support? Can they commit to the expected time? Are there upcoming projects or commitments that would make championing difficult in the near term?

Make it easy to decline or defer. Some people might be excellent champions, but now isn't the right time. Better to wait for the right timing than recruit someone who isn't ready to engage effectively.

Defining Roles and Responsibilities

Champions need clarity about what's expected of them and what's not. Vague role definitions create confusion, frustration, and inconsistent performance.

Core Responsibilities

Define a clear set of core responsibilities that all champions are expected to fulfil. These form the foundation of what it means to be a champion in your programme.

Typical core responsibilities might include:

- ✓ Acting as the security point of contact for their team or domain. When colleagues have security questions or concerns, the champion is the first person they ask. The champion either answers directly or knows who to ask for help.
- ✓ Participating in security-relevant activities within their team. This includes design reviews, code reviews, architecture discussions, incident responses, or other contexts where security considerations matter. Champions ensure security

Create Selection Criteria, Not Barriers

Selection conversations aren't about excluding people but ensuring mutual fit. Have clear criteria for what you're looking for but apply them flexibly. Someone who's missing one characteristic but is exceptionally strong in others may be worth recruiting anyway. Someone who meets all criteria on paper but has no genuine interest won't succeed. Use criteria as a guide for good conversations, not as rigid gatekeeping.

thinking is present in these activities.

- ✓ Engaging with the champions community. Attending champion meetings, participating in discussion channels, and contributing to shared learning. Champions aren't isolated individuals but part of a network that learns and supports each other.
- ✓ Completing development activities. Whatever training, workshops, or learning experiences you provide, champions are expected to participate. They can't be effective without developing capability.

Keep this list focused. If everything is a core responsibility, nothing is. Champions need to know what's truly essential versus what's optional or aspirational.

Optional Activities

Beyond core responsibilities, champions may engage in various optional activities based on their interests, capacity, and expertise. Make these clearly optional rather than implicit expectations.

Optional activities might include:

- ☞ Leading workshops or training sessions for their teams. Some champions enjoy teaching and want to develop these skills.

Others are less comfortable presenting or lack time. Both are fine.

- ☞ Contributing to security standards or policy development. Some champions want to be involved in the organisational security strategy. Others prefer to focus on their teams. Both are valuable.
- ☞ Mentoring newer champions. Experienced champions can accelerate the development of newer champions. But this requires time and inclination. Don't expect all experienced champions to mentor.
- ☞ Participating in working groups or special projects. These provide opportunities for deeper involvement and skill development but require additional time commitment beyond core responsibilities.
- ☞ Being explicit about what's optional prevents champions from feeling guilty about not doing everything. It also helps you identify champions' interests and strengths so you can match people to opportunities appropriately.

Boundaries and Escalation

As important as defining what champions do is defining what they don't do. Clear boundaries prevent champions from taking on inappropriate responsibilities or struggling with situations beyond their capability.

Champions are not security team members. They don't conduct penetration testing, coordinate incident response, or make final security decisions on high-risk matters. They bring security thinking to their contexts but remain part of their primary teams.

Champions are not decision-makers for complex or high-stakes security issues. They should escalate to the security team when issues are beyond their expertise, when risks are significant, or when coordination across teams is needed.

Champions are not responsible for enforcing security policy. They help their teams understand and comply with security requirements, but enforcement rests with the security and management teams.

Define clear escalation paths. When should champions escalate to the security team? What types of issues require immediate escalation versus just flagging for future attention? How do champions escalate effectively?

The Responsibility Trap

Enthusiastic champions sometimes take on more responsibility than is appropriate, either because they feel obligated or because they enjoy the work. This can lead to burnout, decisions beyond their authority, or champions stepping into roles that should remain with the security team. Preventing this requires explicit boundaries and reminding champions that effectiveness comes from operating within their defined scope, not from expanding into every security activity.

Building Community and Connection

Individual champions matter, but the champion community matters more. A strong community of practice fosters peer learning, sustains motivation, and disseminates knowledge effectively.

Creating Connection Points

Champions need regular opportunities to connect with each other, not just with programme leadership. These connections build relationships, enable learning, and create a sense of shared identity.

Regular meetings or gatherings. Most programmes have some form of regular champion meeting. These work best when they're valuable enough that champions want to attend rather than endure mandatory sessions.

Effective champion meetings aren't status updates or top-down broadcasts from the security team. They're interactive sessions where champions learn from one another, discuss challenging scenarios, share solutions to common problems, and develop shared capabilities.

Alex runs champion meetings quarterly rather than monthly: *"We found monthly meetings felt obligatory and often lacked substance. Quarterly meetings give us time to plan meaningful content, including hands-on workshops, case-study discussions, external speaker sessions, and deep dives into emerging threats. Champions actually look forward to these rather than viewing them as calendar burdens."*

Discussion channels. Digital spaces where champions can ask questions, share discoveries, and learn from each other daily. These channels are often more valuable than formal meetings because they're available when champions need help, not just during scheduled sessions.

Effective channels require active participation from programme leadership initially to model behaviours and demonstrate value. As the community matures, champions increasingly help each other without needing programme leadership involvement in every discussion.

Social connections. Not everything needs to be work-focused. Creating opportunities for champions to connect personally strengthens the community. This might be social time before or after meetings, shared meals, informal virtual coffee chats, or non-security channels where champions can share interests and build relationships beyond their security roles.

Facilitating Peer Learning

The champion community holds vast collective knowledge that exceeds what any individual or the security team possesses. Effective programmes make this knowledge accessible and actionable.

Knowledge-sharing sessions where champions present on the topics they're working on. A champion who implemented security testing automation shows others how they did it. A champion who successfully influenced a resistant stakeholder shares their approach. These sessions transfer practical knowledge in context from people who understand the real constraints others face.

Problem-solving forums where champions bring current challenges and workshop solutions together. "*I'm trying to introduce threat modelling in my team, but they see it as bureaucratic. How have*

others approached this?" The community's collective experience provides multiple perspectives and proven approaches.

Pairing and mentoring connect champions with different levels of experience or expertise. A new champion pairs with an experienced champion to learn how they approach code reviews. A champion who's an expert in cloud security mentors one who's building that capability.

Building Shared Identity

Beyond practical learning and support, champions benefit from shared identity. Being a champion means something. It's not just an additional task but a role with meaning and a sense of belonging.

This identity forms through shared experiences, inside jokes, common challenges, mutual support, and recognition of collective

Make It Safe to Not Know

The best champion communities are ones where people feel comfortable admitting uncertainty and asking "basic" questions. If champions fear looking incompetent, they won't seek help and won't share the struggles that lead to breakthrough learning. Programme leaders set this tone by acknowledging their own uncertainties, by celebrating good questions, and by gently redirecting anyone who makes others feel foolish for asking.

impact. It's reinforced through visible symbols like champion badges or profiles, through programme rituals and traditions, through stories of champion impact that get told and retold.

Strong identity sustains engagement when motivation wavers. Champions stay involved partly because being a champion is part of how they see themselves and how others see them. They don't want to let down the community they're part of.

Creating identity isn't about manufacturing culture through forced team-building or corporate branding exercises. It emerges from genuine shared experience and mutual respect. Programme leaders facilitate this by creating conditions where champions work together meaningfully, support each other genuinely, and achieve things they're proud of collectively.

Establishing Communication Rhythms

How champions communicate internally and with the security team shapes programme effectiveness. Good communication keeps everyone informed, enables coordination, and maintains connection. Poor communication creates confusion, duplication, and isolation.

Internal Champion Communication

Champions need to communicate regularly, but not so much that it becomes burdensome.

Consider multiple channels for different purposes. An "*announcements*" channel for programme-wide information that everyone needs to see. A "questions" channel where champions seek quick help. Topic-specific channels for champions with particular interests or specialisms. A "*random*" channel for social connection and informal discussion.

Different people have different communication preferences. Some champions are very active in async channels and benefit from daily interaction. Others prefer to check in less frequently and participate in structured meetings.

Some are comfortable with video calls, others prefer text-based communication. Allow for this variation rather than assuming everyone engages the same way.

Set expectations about response times. For urgent issues, how quickly should champions expect responses? For routine questions, what's reasonable? Without clear expectations, some champions will expect immediate responses and become frustrated by delays, whilst others will hesitate to ask for fear of bothering people.

Champion-to-Security Team Communication

The relationship and communication between champions and the security team require particular attention. This is where champions get support, where security concerns get escalated, and where organisational security knowledge flows.

Champions need clear paths to reach the security team when they need help. Some programmes have dedicated office hours when security team members are available for champion questions. Others have a specific channel or ticketing system for champion requests. Whatever the mechanism, it must be responsive enough that champions feel supported rather than ignored.

The security team also needs information from champions: visibility into what's happening across teams, early warnings about potential

Signal-to-Noise Ratio Matters

If your champion channels are full of noise (automated notifications, tangential discussions, redundant information), engaged champions will tune out and miss important content. Protect your channels' value by being selective about what gets posted. Use separate channels for automated alerts so champions can choose whether to monitor them. Keep discussions focused and redirect off-topic conversations. Champions will engage more when the content is consistently valuable.

issues, and feedback on security requirements and processes. But this can't feel like surveillance or reporting for its own sake. Communication should primarily serve champions' needs, with security team visibility as a benefit rather than the main purpose.

Regular check-ins between programme leadership and individual champions help maintain these relationships. These don't need to be formal or lengthy, but they should happen often enough that issues are caught early and champions feel connected to programme leadership.

External Communication

Beyond internal champion and security team communication, consider how champions communicate about security to their teams and the broader organisation.

Provide champions with communication support. When significant security issues or changes arise, give champions talking points or FAQs they can use in team discussions. When security requirements change, help champions explain why those changes matter to their specific contexts. Champions shouldn't be left to translate complex security communications alone.

Create mechanisms for teams and managers to provide feedback about their champions and the programme overall. This feedback

helps identify what's working, what's not, and where champions need additional support.

Sustaining Engagement Over Time

The biggest challenge in champions programmes isn't launch but sustainability. Initial enthusiasm fades. Competing priorities emerge. Champions who were excited in month one struggle to stay engaged in month twelve.

Creating Ongoing Value

Champions sustain engagement when their activities deliver genuine value for both their personal development and their teams.

Personal development value comes from learning security skills, developing professional capabilities, and gaining organisational visibility. Champions should demonstrably become more knowledgeable about security, more skilled in influencing and communicating, and more visible to leadership. These benefits justify the time investment even when security work itself is challenging.

Team value comes from champions making security easier for their teammates rather than harder. Teams with effective champions should experience less friction with security, fewer surprises late in development, and faster resolution of security questions. If teams

view their champion as enabling rather than constraining, champions' work feels valued.

Organisational recognition reinforces both types of value. When champions' contributions are visible and acknowledged, they see that their work matters. When they're invisible or taken for granted, motivation declines.

The Value Exchange

A technology company tracked why champions disengaged over their first year. The primary factor wasn't time commitment or difficulty but perceived value. Champions who felt they were developing valuable skills and making a meaningful impact stayed engaged even when time-pressed. Champions who felt they were just attending meetings and completing tasks disconnected from real impact, disengaged despite having available time. The lesson: value sustains engagement more than convenience.

Maintaining Manageable Scope

Champions disengage when demands feel unsustainable. The role that seemed reasonable at recruitment becomes overwhelming as expectations creep upward. Champions can't say no without feeling they're failing, so they quietly disengage instead.

Protect champions from scope creep. Be explicit about what's expected and what's optional. When new opportunities or responsibilities arise, discuss whether to add them or reduce existing responsibilities to accommodate them. Champions need permission to maintain boundaries around their commitment.

This requires programme leadership that advocates for champions when organisational demands become excessive. The security team wants champions to do more. Engineering leadership wants broader champion coverage. Product teams want faster response times from champions. All understandable desires, but collectively they can overwhelm champions.

Refreshing Programme Elements

Even well-designed programmes get stale. The monthly champions meeting that was engaging initially becomes routine. The training that was valuable twelve months ago no longer challenges experienced champions. The communication patterns that worked early don't scale or don't maintain interest.

Refresh programme elements periodically based on feedback and observation. Change meeting formats when they're no longer engaging. Introduce new development opportunities as champions

advance. Update programme structure when it no longer fits organisational reality.

Champions themselves are your best source for improvement ideas. They experience the programme directly and often see opportunities for enhancement before programme leadership does. Create channels for champion feedback and demonstrate that feedback leads to actual change.

Measuring Network Health

You need ways to assess whether your network is functioning effectively. Not just whether you have enough champions, but whether those champions are engaged, capable, and valuable.

Activity Metrics

Track tangible champion activities as basic health indicators. How often are champions attending meetings or training? How often do they participate in channels or respond to questions? How many security reviews or consultations are they involved in?

These metrics don't tell you whether champions are effective, but they tell you whether champions are engaged. Declining activity often precedes eventual dropout, so tracking activity helps you identify problems early.

Capability Development

Assess whether champions are developing security capability over time. This can be formal (through assessments or certifications) or informal (through observation of how champions handle increasingly complex situations).

Are champions who've been in the role for six months more confident and capable than new champions? Can they handle questions that they would have escalated initially? Do they provide more sophisticated input in security discussions? If champions aren't developing capability, your programme isn't delivering development value.

Team and Stakeholder Feedback

The people who work with champions provide a crucial perspective on effectiveness. Do teams value their champion's contribution? Do

The Annual Refresh

Plan an annual programme refresh where you systematically review what's working and what's not. Survey champions about their experience. Analyse participation patterns. Compare the current programme design to how champions engage. Make deliberate changes based on this review. This prevents gradual programme degradation whilst signalling that you're continuously improving based on champion experience.

managers see improvements in team security with champions? Does the security team view champions as helpful collaborators?

Regular feedback from these stakeholders validates that champions are having the intended impact whilst identifying specific champions who may need additional support or development.

Retention and Churn

Track how long champions remain engaged and why they leave. Healthy programmes retain most champions for at least a year and lose them primarily to role changes rather than disengagement.

If you're losing significant numbers of champions within their first six months, something about your recruitment, onboarding, or support isn't working. If experienced champions are leaving because they're frustrated or feel unsupported, your programme's sustainability needs attention.

Metrics That Matter

An engineering organisation tracked extensive metrics for its champions programme, including the number of champions, training completion rates, channel participation, meeting attendance, and the number of security tickets handled. All showed healthy numbers. Yet the programme wasn't having an impact. They added one new metric: "How many design decisions were influenced by champion input last quarter?" That revealed the problem. Champions were doing activities but not influencing outcomes. They refocused champion activities on high-leverage interactions rather than activity volume. Impact increased even as some activity metrics decreased.

Starting Small and Scaling Thoughtfully

The temptation when designing a champions network is to plan for your end state: complete organisational coverage, sophisticated structures, comprehensive capabilities. Resist this temptation.

Start smaller than you think you should. Recruit fewer champions initially than your complete coverage would require. Focus on specific teams or domains where you're confident you can demonstrate value. Build the foundations of your programme with a manageable network before scaling.

This approach has multiple advantages. You can provide intensive support to initial champions, helping them become effective quickly.

You can learn what actually works in your context rather than committing to structures based on theory. You can demonstrate value to stakeholders before asking for resources to scale. You can build a strong community foundation with your initial cohort, who then help onboard and support later champions.

Programme failures often come from trying to do too much too quickly. You recruit aggressively to hit coverage targets, but can't support all those champions effectively. They struggle, they disengage, and the programme develops a reputation for ineffectiveness. Recovering from that is harder than starting small and building deliberately.

Louise launched a champions programme at a healthcare organisation: *"We identified 45 teams that needed champion coverage based on our risk assessment. Instead of recruiting 45*

Pilot, Prove, Scale

Treat your initial launch as a pilot regardless of your long-term vision. Set explicit pilot goals and timeframes. Plan to evaluate and adjust before scaling. This gives you permission to start imperfectly and to make changes based on what you learn. It also manages stakeholder expectations. Frame your initial launch as deliberately limited so you can build something that works rather than deliver complete coverage immediately. Stakeholders generally accept this if you're clear about your reasoning and your scaling plans.

champions immediately, we started with 8 champions in the highest-priority areas. We invested heavily in supporting those 8. They became effective quickly and visibly improved security in their teams. After six months, we expanded to 15 champions, then to 25 over the next year. Some of our initial champions helped recruit and train newer champions. Two years in, we have 35 highly engaged champions covering our most critical areas. We could have recruited 45 initially, but they wouldn't have been as effective, and many would have dropped out."

Adapting to Your Reality

This chapter has covered a lot of ground: assessing context, structuring networks, recruiting champions, defining roles, building community, establishing communication, and sustaining engagement. The details matter, but don't lose the fundamental principle.

Your Security Champions programme should be designed for your organisation's specific context, culture, and needs. Not adapted reluctantly from a generic template, but built from the ground up to work in your reality.

Take the principles and frameworks presented here, then customise them. Talk with potential champions about what would work in their

world. Pay attention to what your organisation already does well and build on that. Observe what creates friction in your culture and avoid it. Test your assumptions with small pilots before committing to a large-scale rollout.

The programme that succeeds isn't the one that looks most impressive on paper. It's the one that works in practice, that fits how people actually operate, that solves real problems rather than theoretical ones, that sustains over time because it delivers genuine value to champions and their teams.

You're not building a programme despite your organisation's quirks and constraints. You're building a programme that succeeds precisely because it's designed around them.

Now that you understand how to design a programme that fits your context, the next chapter explores how to develop and sustain champions over time, ensuring they build capability and remain engaged long after initial enthusiasm fades.

Chapter 5: Developing and Sustaining Champions

The hardest part of building a Security Champions programme isn't launching it. It's keeping it alive six months later when the initial excitement has worn off, when competing priorities have emerged, when champions realise that this actually requires ongoing effort.

Most programmes that fail don't collapse dramatically. They fade. Champions stop attending meetings because they're too busy. The Slack channel goes quiet except for automated security notifications nobody reads. Training sessions get rescheduled, then cancelled. Within a year, the programme exists mainly in organisational charts and forgotten wiki pages.

This chapter addresses the fundamental challenge of Security Champions programmes: sustaining engagement over time. We'll explore how to systematically develop champions' capabilities, how to create value that motivates continued participation, and how to build programme infrastructure that supports rather than burdens champions.

Because the real measure of your programme isn't how many champions you recruit. It's how many are still actively engaged twelve months later.

The Development Paradox

Here's the paradox every programme leader faces. Champions need development to be effective. But development activities take time away from their primary roles. And that time commitment is precisely what makes champions drop out.

Sarah, who runs a champions programme at a financial services firm, described her experience: "We built this comprehensive training curriculum. Six modules covering everything a champion needed to know. It was excellent content. But we lost 40% of our champions before they completed it. They weren't learning enough to feel confident, but they were spending enough time to feel overwhelmed."

The solution isn't less development. Champions who don't develop capability become ineffective and frustrated. The solution is development that creates immediate value while building long-term capability.

Think about how skilled craftspeople develop expertise. They don't complete theoretical training before starting to practise. They work

on real projects from the beginning, developing capability through guided practice on increasingly complex work. Their development creates value from day one by contributing to real projects while they learn.

Your champions' development should follow the same principle. Every development activity should either solve a problem they're currently facing or prepare them for work they'll do next week, not next quarter.

The Capability Progression Model

Champions develop through three overlapping phases, each building on the previous whilst preparing for the next. Understanding these phases helps you design development activities that match where champions actually are, not where you wish they were.

Phase One: Foundational Competence (Months 1-3)

In their first three months, champions need to develop basic security literacy and learn how to spot common issues in their domain. They're not expected to solve complex problems independently. They need to recognise when security matters and know who to ask for help.

Development in this phase focuses on pattern recognition. What does insecure code look like in their technology stack? What processes commonly introduce risk? What questions should they ask during design reviews? These aren't abstract principles but concrete examples drawn from actual incidents and near-misses in your organisation.

Jamie, a newly recruited champion in a product team, described her early development: "*The security team gave me a list of the top ten issues they found in code reviews last quarter. Actual examples from our codebase with explanations of why they mattered. When I reviewed the code afterwards, I knew what to look for because I'd seen the patterns. I caught three issues in my first week.*"

That's foundational competence in action. Not comprehensive security knowledge, but enough practical capability to add immediate value whilst building confidence.

The key development activities in this phase are short and highly practical. Lunch-and-learn sessions analysing recent incidents. Guided code review where experienced champions explain what they're looking for. Shadowing sessions where new champions observe security conversations in practice.

Each activity should take less than an hour and should result in something the champion can apply that same week. They're

learning by doing, with safety nets provided by more experienced champions and the security team.

The Confidence Gap

A technology company discovered that new champions often stopped engaging around week six, right when they should have been gaining momentum. Exit interviews revealed champions felt they'd learned enough to realise how much they didn't know, but not enough to feel confident contributing. They worried about giving wrong advice and chose silence over risk. The solution was explicit "learning licence" messaging: "For your first three months, you're expected to ask questions, make mistakes, and learn. Your job isn't to be the expert but to become one." Retention improved dramatically.

Phase Two: Independent Practice (Months 3-6)

After three to six months, champions should be handling routine security matters independently. They're identifying common issues, answering straightforward questions from their teams, and making low-risk security decisions without constant validation.

Development in this phase focuses on judgment. When is an issue serious enough to escalate? How do you balance security concerns against delivery pressure? What's the difference between a

vulnerability that needs immediate attention and one that can be addressed in the next sprint?

This is where champions often struggle. Technical knowledge is relatively straightforward to acquire. Judgement requires experience and reflection. You can't simply tell champions when to escalate or how to balance competing concerns. They need to develop that capability through guided practice and feedback.

Mark runs a champions programme at a software company. His approach to developing judgment is instructive: "*We have office hours twice a week where champions can bring questions. Not just technical questions but judgment calls. 'I think this could be a problem, but I'm not sure if it's serious enough to delay the release.' We talk through how to assess it. They start recognising the patterns.*"

He also created a private channel where champions share decisions

Create a Decision Journal

Encourage champions to maintain a simple decision journal where they record security decisions they make, their reasoning, and outcomes. Reviewing this journal quarterly helps champions see their own progression and identify patterns in their decision-making. It also provides material for coaching conversations and helps you identify common challenges across your champion community.

they're unsure about. Other champions and security team members provide feedback not only on whether the decision was correct but also on the reasoning behind it. Over time, champions internalise that reasoning process.

The development activities in this phase look different from those in Phase One. Less time in training sessions, more time in mentoring relationships. Regular case-study discussions in which champions analyse real scenarios from the organisation. Peer learning where champions with different specialisms share expertise.

Most importantly, champions in this phase start teaching others. They present at team meetings, run workshops for new joiners, and contribute to documentation. Teaching reinforces learning whilst building their credibility within their teams.

Phase Three: Strategic Contribution (Months 6-12+)

After six to twelve months, effective champions move beyond tactical issues to strategic contributions. They're influencing architectural decisions, shaping processes, and identifying systemic security improvements. They're not just reacting to problems but proactively preventing them.

Development in this phase focuses on systems thinking and influence. How do security concerns interconnect across the

organisation? How do you build support for changes that improve security but require effort from multiple teams? How do you make the case for security investments when resources are constrained?

These capabilities matter because experienced champions often have more influence over organisational security than the security team itself. They understand the business context, they have credibility with delivery teams, and they know how to navigate organisational politics. But they need development to use that influence effectively.

Rachel, a champion who'd been in the role for two years, described her progression: *"Initially, I was finding bugs and asking security questions. Important, but tactical. Now I'm involved in architecture reviews, I'm pushing for security requirements to be part of our product planning, and I'm training new champions. The security team treats me as a peer, not someone they need to educate. That required a different kind of development."*

Her organisation provided that development through structured opportunities to work on strategic projects. Champions collaborated with the security team on developing security standards. They participated in incident response exercises. They presented at architecture review boards. Each experience developed their capability whilst demonstrating their strategic value.

The development activities in this phase are less structured but more substantial. Champions might take on a project to improve security testing across multiple teams, requiring them to analyse current practices, design improvements, and build support for change. They might mentor less experienced champions, helping them develop their leadership and communication skills.

Not every champion will reach this phase, and that's fine. Some champions prefer to focus on tactical contributions within their teams and are extremely valuable doing so. But for those who want to develop further, the programme should provide pathways for strategic contribution.

The Expertise Plateau

After about eighteen months, some champions reach an expertise plateau where they've mastered the security aspects relevant to their role but aren't being challenged to grow further. These champions often disengage or leave the programme unless you provide new development opportunities. Options include rotating them to mentor newer champions, involving them in programme leadership, assigning them cross-domain projects, or supporting them in pursuing security certifications. The key is recognising that development needs don't stop once someone becomes proficient.

Building Capability Through Community

The most effective development doesn't happen in training sessions. It happens through everyday interactions, where champions learn from one another, share solutions to common problems, and build collective expertise.

This is why community matters more than curriculum. A strong community of practice creates continuous learning opportunities that are contextual, relevant, and sustainable. Champions learn by observing how others handle similar situations, by discussing challenging scenarios, and by sharing resources and tools.

Creating Spaces for Learning

Development through community requires intentionally designing spaces where learning happens naturally. These spaces need to lower the barriers to asking questions, sharing uncertainty, and admitting mistakes.

Consider how most corporate communication channels work. Someone posts a question. They wait. Eventually, someone responds. Maybe a conversation develops, maybe not. The channel serves as a repository more than a community.

Contrast that with how effective champion communities function. Questions get responses within minutes, often from multiple champions offering different perspectives. Discussions are rich because people build on each other's ideas. When someone shares a challenge, others contribute similar experiences and solutions.

The difference isn't the platform. It's the norms and practices that govern how people interact.

Alex, who manages a champions programme at a technology company, described how they built these norms: *"We explicitly modelled the behaviour we wanted. When champions asked basic questions, senior people answered enthusiastically, without any hint that the questions were obvious. When someone shared a mistake, we thanked them for the learning opportunity. When discussions got technical, we paused to explain jargon. Within a few months, the*

The 24-Hour Response Commitment

Programme leaders and experienced champions should commit to responding to questions in community channels within 24 hours, even if the response is "I don't know but I'll find out" or "Let's discuss this in office hours." This commitment signals that the community is active and responsive, which encourages others to participate. Dead channels where questions go unanswered train people not to ask, killing the community's value.

community was self-reinforcing those norms."

They also structured interactions to encourage participation. Weekly challenges where champions solved realistic security scenarios and shared their approaches. Monthly "*what I learned*" threads where champions reflected on recent experiences. Dedicated channels for specific topics so discussions stayed focused and findable.

The goal wasn't to create more noise but to create more signal. Champions could quickly find answers, see how others approached similar problems, and learn from the community's collective expertise.

Leveraging Peer Learning

Champions bring diverse expertise. Some are experts in application security, others in infrastructure security, and still others in secure development practices. Some have deep technical knowledge, others understand organisational dynamics better. This diversity is a strength if you design opportunities for peer learning.

The simplest approach is pairing. When a champion faces a challenge outside their expertise, pair them with someone who has relevant experience. They solve the problem together whilst the first champion develops a new capability.

Sarah's programme does this systematically: "*We maintain a skills matrix showing each champion's areas of expertise. When champions need help, we connect them with someone who has the relevant experience. They work together, which solves the immediate problem while building the first champion's capability. Over time, everyone develops broader expertise.*"

More structured peer learning happens through champion-led workshops. Rather than the security team running all training, champions with specific expertise teach others. A champion who's an expert in API security runs a workshop on common API vulnerabilities. A threat modelling champion facilitates a session on threat analysis techniques.

This approach has multiple benefits. The champion leading the workshop reinforces their own expertise through teaching. Other champions learn from someone who understands their context because that person works in a similar role. The security team's training burden reduces whilst overall capability increases.

Some programmes create peer-review processes in which champions review each other's work. Security designs get reviewed by champions from other teams. Secure coding practices get shared and critiqued. This creates accountability whilst building expertise across the community.

Curating Collective Knowledge

As your champions community matures, it accumulates substantial knowledge: solutions to common problems, tools that work well, processes other teams have successfully adopted, and lessons from incidents and near-misses.

This knowledge becomes invaluable if it's accessible. But most organisations are terrible at knowledge management. Information lives in chat archives nobody searches, in documents nobody remembers exist, in the heads of people who've moved to other roles.

Effective programmes curate this knowledge deliberately. Not by trying to document everything, which creates unusable reference material nobody maintains. But by capturing the most valuable insights in findable, actionable formats.

At a minimum, you need a small set of living documents that champions actually use. A troubleshooting guide for common issues. A collection of secure coding examples in your tech stack. A decision framework for when to escalate concerns. A glossary of security terms in language that makes sense for your organisation.

These documents should be owned by the champions community, not the security team. Champions update them when they discover

better approaches. They add examples from recent projects. They clarify sections that caused confusion. The documents remain relevant because the people who use them maintain them.

More sophisticated approaches involve building searchable repositories of past discussions, tagging content by topic and context, creating curated reading lists for different specialisms, and maintaining a library of how security issues were handled.

The goal isn't comprehensive documentation. It ensures that when a champion faces a situation, they can quickly find relevant examples of how similar situations have been handled. That accelerates learning whilst preventing the same mistakes from being repeated across multiple teams.

The Wiki Graveyard

Many programmes create elaborate wikis full of security information that nobody ever reads. The problem isn't the information quality but the delivery mechanism. Static wikis require champions to know what to search for and wade through generic content to find relevant bits. Better approach: create targeted, context-specific resources that champions encounter when they need them. A "secure coding checklist for React" that lives in the React repository. A "threat modelling guide for API design" that the architecture team references. Knowledge that's embedded in workflows gets used. Knowledge that lives in a separate wiki doesn't.

Creating Sustainable Engagement Models

Development activities are necessary but not sufficient for sustaining engagement. Champions also need to see that their participation delivers value for both their personal development and their teams. Without that value, no amount of interesting training will maintain motivation over time.

This means designing engagement models that work with champions' realities rather than imposing additional burdens on already busy professionals.

Embedding Security Champion Work in Existing Workflows

The most sustainable programmes integrate champion activities into work that champions are already doing, rather than creating separate security work on top of their normal responsibilities.

Consider code reviews. Most development teams already do them. Rather than expecting champions to conduct additional security-focused reviews, train them to incorporate security considerations into their regular reviews. They're doing the work anyway; they're just doing it with a security lens.

The same principle applies to design discussions, sprint planning, incident responses, and other standard workflows. Champions

contribute security thinking within existing processes rather than bolting on separate security processes.

Emily runs a champions programme at a software company. Her insight: *"When we asked champions to attend separate security design reviews, attendance was poor, and champions felt burdened. When we trained them to raise security considerations in their normal design discussions, adoption was high because we hadn't added work. We'd enhanced the work they were already doing."*

This approach has another benefit. Security becomes integrated into how teams work rather than a separate concern they address occasionally. Over time, secure practices become the norm as champions consistently reinforce them in everyday workflows.

Map the Integration Points

*List all the regular activities in your champions' workflows: stand-ups, code reviews, design sessions, sprint planning, retrospectives, and incident reviews. For each activity, identify one way security thinking could be naturally integrated. Don't try to integrate security into everything immediately. Pick two or three high-value integration points and help champions incorporate security thinking t*here first. Add more integration points gradually as champions develop capability and confidence.

Right-Sizing Time Commitments

One of the fastest ways to kill a champion programme is to underestimate the time commitment required. Champions join enthusiastically, discover it takes more time than they expected, feel guilty about not meeting expectations, and quietly disengage.

Be explicit about time requirements from recruitment onwards. Don't oversell the role as "*just a few hours a month*" when it realistically requires more. Champions who set realistic expectations are more likely to sustain engagement than those who feel misled.

For most programmes, active champions invest four to eight hours per month on champion activities. This includes time spent on security reviews, attending champion meetings, contributing to the community, and personal development. Some months require more time, others less, but that's a reasonable average.

Some champions will invest more time because they're passionate about security or want to develop expertise. That's excellent, but it shouldn't be the baseline expectation. Your programme should function effectively even if champions are only committing the minimum expected time.

Also, recognise that time commitment varies by role and seniority. A senior architect can integrate security considerations into the design

reviews they already facilitate with minimal additional effort. A junior developer reviewing code needs more dedicated time to research security issues they encounter. Design your expectations accordingly.

The Burnout Pattern

A healthcare technology company tracked champion engagement over time and discovered a concerning pattern. Champions were most active in months 2-4, then activity dropped sharply around months 5-6. The investigation revealed that enthusiastic champions were overcommitting early, spending 10-15 hours per month on champion activities, and then burning out when that proved unsustainable alongside their primary responsibilities. They reduced baseline expectations to 4-6 hours per month and explicitly told champions to maintain that pace rather than sprint. Sustained engagement improved significantly.

Recognising Contribution Appropriately

Recognition matters, but it's more subtle than most programme leaders assume. Generic "*thanks for your contribution*" statements at team meetings don't sustain motivation. Neither do token rewards like security-themed t-shirts or stickers.

What sustains motivation is recognition that acknowledges specific contributions and demonstrates genuine appreciation of the impact those contributions had.

When a champion identifies a significant vulnerability, don't just thank them privately. Tell their manager, tell their team, tell the champions community. Explain what they caught and why it mattered. Make their contribution visible.

When champions develop new capabilities, create opportunities for them to demonstrate those capabilities. Let them present at architecture reviews, contribute to security policy development, and mentor other champions. Recognition through responsibility signals that you trust their expertise.

Some organisations incorporate champions' work into performance reviews and promotion criteria. This requires management support but sends a strong message that security contribution is valued alongside other professional accomplishments.

Financial rewards are complex. In some organisational cultures, providing compensation for champion activities makes sense and reinforces their value. In others, it undermines intrinsic motivation by making security work feel like a paid side project rather than an important professional contribution. Know your culture.

The most powerful recognition is often the simplest: public acknowledgement of specific contributions in ways that enhance champions' professional reputation. "*Emily identified a design flaw*

that would have exposed customer data. Her security thinking during architecture reviews is exactly why this programme matters."

The Recognition Portfolio

Help champions build a "*recognition portfolio*" documenting their contributions: vulnerabilities they've identified, improvements they've driven, people they've trained, and presentations they've delivered. This portfolio serves two purposes. It helps champions see their own progress and impact, helping them maintain motivation during challenging periods. It also provides concrete evidence of their contributions for performance reviews and career development discussions.

Providing Clear Progression Paths

Champions who stagnate often disengage. If the role feels the same twelve months in as it did on day one, motivation drops. Champions need to see progression, either within their champion role or through it into other opportunities.

This doesn't mean creating elaborate hierarchies. "*Junior champion, champion, senior champion, lead champion*" structures often create bureaucracy without adding value. But champions should have

opportunities to take on more responsibility and develop new capabilities as they grow.

Simple progression structures work well. New champions focus on their own teams. Experienced champions might mentor newer champions or work on programme-wide initiatives. Highly experienced champions might lead working groups, contribute to security strategy, or take on formal security team roles.

Make these progression opportunities visible. When champions see peers taking on interesting challenges and developing valuable expertise, they're motivated to do the same. When progression paths are unclear, champions assume their development has plateaued.

Michael's organisation handled this particularly well: *"We publish stories about champions' progression. How they started, what they've contributed, where they are now. Some champions moved into security team roles. Others became security leads in their departments. Others advanced in their primary roles because their security expertise set them apart. Showing these paths helps champions see possibilities."*

Managing Champion Churn

Despite your best efforts, champions will leave the programme. People change roles, join different organisations, and shift focus to

other priorities. Some attrition is inevitable and healthy. But managing it well ensures continuity and minimises disruption.

Planned Transitions

The most manageable departures are planned. A champion decides to step down, gives reasonable notice, and helps transition their responsibilities. Your programme should make this easy and graceful.

Avoid creating cultures where leaving the programme feels like failure or betrayal. Champions should feel comfortable saying, "I've committed two years, developed my capability, and now want to focus on other areas." That's a success, not a problem.

When champions do transition out, treat it as an opportunity. Thank them for their contribution, document what they learned, and identify what worked well and what could improve. Exit conversations with departing champions often provide your best feedback on programme health.

Also create alumni networks. Former champions remain valuable even after they've stepped down. They can mentor current champions, provide advice on specific issues, and serve as programme advocates. Don't lose those relationships simply because someone's no longer an active champion.

Unplanned Departures

More challenging are champions who disengage without an explicit transition. They stop attending meetings, stop responding in channels, and effectively drop out whilst nominally remaining champions.

When you notice this pattern, reach out to each person individually. Often, there's a salvageable situation. The champion is temporarily overwhelmed with other work. They're uncertain about their contribution. They encountered a situation that frustrated them. A conversation can often re-engage them or help them transition out gracefully.

If a champion has been disengaged for two months despite outreach attempts, remove them from the active champions list. Not punitively, but pragmatically. An organisation chart showing fifty champions when fifteen are actually active undermines programme credibility.

Do this with care, though. Sometimes champions disappear, then resurface months later when their situation changes. Leave the door open for them to rejoin if their circumstances permit.

The Check-In Cadence

Don't wait until champions are fully disengaged to reach out. Have structured quarterly check-ins with all champions where you ask about their experience, challenges, and future intentions. These conversations catch early warning signs whilst champions are still engaged enough to course-correct. They also signal that you care about champions' experience, not just their productivity.

Knowledge Transfer and Continuity

The biggest risk of champion churn isn't losing numbers; it's losing knowledge and relationships. A long-serving champion knows their team's systems, risks, and dynamics. When they leave, that contextual knowledge disappears unless it's been transferred.

Build knowledge transfer into your programme design. Champions should document their team's common security issues, security decisions, and improvement priorities. Not elaborate documentation, but sufficient context that a replacement champion can be effective quickly.

Pair newer champions with experienced champions in similar domains. When the experienced champion eventually transitions out, the newer champion has already developed relevant expertise and relationships.

For critical teams, consider having two champions rather than one. This provides redundancy when one champion leaves and accelerates development for both champions through peer collaboration.

The Key Person Risk

A manufacturing company discovered its entire API security knowledge resided with one champion. When she left the company for a new role, there was no champion who understood their API architecture, the security decisions made, or the ongoing vulnerabilities they were tracking. It took three months to rebuild that knowledge. After that incident, they implemented mandatory knowledge documentation for all champions covering critical systems and ensured that at least two champions were familiar with each critical area.

Sustaining Your Own Momentum

Running a Security Champions programme is demanding work, especially in the first year when you're building foundational elements whilst maintaining day-to-day operations. Programme leaders burn out just like champions do.

You need sustainable practices for yourself, not just for your champions.

Building Your Support Network

Don't try to run the programme alone. Even if you're the designated programme leader, you need peers who understand the challenges and can provide perspective when you're stuck.

Connect with other programme leaders inside your organisation if multiple programmes exist. They face similar challenges around engagement, recognition, and executive support, even if their domains differ. Learning from each other accelerates everyone's progress.

Also connect with programme leaders at other organisations. The Security Champions community across companies is remarkably generous with sharing lessons, tools, and support. Find that community through conferences, professional networks, or online forums.

Rachel, who built a champions programme from scratch, emphasised this: "*When I felt like I was failing because half my champions weren't engaging, talking to other programme leaders helped me see that was normal. They shared what worked for them, and I adapted those approaches; engagement improved. Without that external network, I would have struggled much longer.*"

Celebrating Incremental Progress

It's easy to focus on everything that's not yet working. The champions who aren't engaged, the teams that haven't recruited champions, the capabilities that aren't fully developed, the programme vision that hasn't been realised.

Acknowledge progress regularly. Each quarter, reflect on what's improved. Champions who are now handling issues they would have escalated three months ago. Teams whose security posture has strengthened through champion involvement. Processes that now include security considerations by default.

These incremental improvements compound. The programme that seems to be progressing slowly in month three often shows dramatic impact by month twelve because all those small improvements have accumulated.

Share these progress stories with your champions, your executive sponsor, and your security team. Not to boast, but to maintain motivation and demonstrate value. Everyone involved needs to see that the effort is producing results.

Knowing When to Adjust Course

Sometimes your programme approach isn't working. Engagement is declining despite your efforts. Champions aren't developing capability effectively. The value you're delivering doesn't justify the effort being invested.

When you see these patterns, adjust. Don't persist with an approach that's clearly failing due to a lack of commitment to your original plan. The best programme leaders are pragmatic experimenters, not rigid planners.

Sarah described her experience*: "Six months in, our monthly champion meetings had become tedious status updates that nobody found valuable. Attendance was dropping. Rather than trying to make the meetings more engaging, we cancelled them. Instead, we held quarterly in-person workshops focused on hands-on skill development and ad hoc video calls when specific issues needed discussion. Engagement improved immediately."*

That kind of course correction requires humility and flexibility. You need to acknowledge what isn't working, gather input on alternatives, make changes, and assess whether those changes improve things. Not every adjustment will succeed, but standing still whilst engagement declines definitely doesn't succeed.

Measuring Sustained Engagement

You need ways to assess whether champions remain engaged over time and whether your development and sustainability practices are effective.

Leading Indicators

Don't wait for champions to formally quit to recognise disengagement. Track leading indicators that signal declining engagement before it becomes terminal.

Attendance at champion meetings or events is trending downward. Participation in champion channels decreases. Response times to questions lengthen. Champions stop volunteering for programme activities. Champions cancel one-on-one sessions repeatedly.

These patterns often emerge gradually, which makes them easy to miss if you're not tracking systematically. A simple dashboard showing participation metrics by champion helps you spot trends early.

When you see declining engagement from individual champions, investigate quickly. Often, there's a specific cause: increased pressure in their primary role, frustration with an aspect of the

programme, or unclear expectations about their contribution. Many of these situations are addressable if you catch them early.

Measuring Capability Development

Track how champions' capabilities develop over time, both to validate your development approach and to demonstrate champions' growing value.

This doesn't require complex assessment systems. Simple, practical measures work better. Can champions now handle issues they would have escalated six months ago? Are they contributing more sophisticated insights in design reviews? Are they helping other teams with security questions?

Qualitative feedback from champions themselves provides valuable insight. Quarterly check-ins where you ask what capabilities they've developed, what they're more confident doing now than before, and what they're still struggling with. These conversations validate development effectiveness whilst helping you identify gaps.

Also gather feedback from the champions' teams and managers. Are they seeing champions contribute more effectively to security? Do they value the champion's security input more than they did initially? This external validation confirms that capability development is translating into practical impact.

Retention Metrics

Ultimately, sustained engagement shows up in retention rates. What percentage of champions are still actively engaged after six months, twelve months, eighteen months?

There's no universal benchmark because champion roles and expectations vary widely. But you should see most champions remain engaged through their first year if your sustainability practices are working. Losing 30-40% of champions in their first six months signals serious problems with your engagement model.

Track why champions leave when they do. Different departure reasons require different responses. Champions leaving because of role changes or organisation exits are inevitable. Champions leaving because they don't see value or feel overwhelmed indicate programme issues you need to address.

Pay particular attention to when champions leave. If most departures happen around three months, your onboarding and early development may be ineffective. If champions typically leave after around twelve months, you may lack opportunities for progression for experienced champions.

The Engagement Dashboard

One programme leader created a simple monthly dashboard tracking five metrics per champion: meeting attendance, channel participation, security reviews completed, questions asked or answered, and hours invested. Champions consistently showing zeros across multiple metrics triggered individual check-ins. This early warning system helped them catch disengagement early and address underlying causes before champions dropped out entirely. The dashboard took 30 minutes per month to maintain, but saved countless hours of reactive recruitment and training.

When Good Programmes Still Struggle

Even well-designed programmes with strong sustainability practices sometimes struggle with engagement. Often, the root causes lie outside the programme itself.

Organisational Context Issues

If your organisation is undergoing a major transformation, sustained engagement in anything beyond immediate priorities becomes difficult. Champions facing redundancy concerns, team restructures, or dramatic strategy shifts understandably focus there rather than on security champion activities.

Similarly, if delivery pressure intensifies substantially, champions may need to step back temporarily. A team rushing to meet a critical deadline can't maintain normal champion engagement during that period.

In these situations, don't fight the context. Acknowledge that champion engagement may decline temporarily, and focus on maintaining a minimum viable level of participation from your most committed champions. When the immediate pressure eases, you can rebuild broader engagement.

Programme-Programme Conflicts

Many organisations run multiple champion or ambassador programmes simultaneously. Developer experience champions, testing champions, accessibility champions, reliability champions, security champions. Each programme wants engaged participants. Collectively, they may ask more than people can reasonably deliver.

If your champions are being pulled in multiple directions, work with other programme leaders to coordinate expectations and reduce duplication. Perhaps some activities can be combined. Perhaps some champions can focus primarily on one programme whilst maintaining lighter engagement in others.

This requires negotiation and compromise, but it's better than competing for the same people's time and creating burnout across all programmes.

Cultural Misalignment

Some organisational cultures simply don't support volunteer-driven improvement programmes. If your organisation has a strong culture of "*that's not my job,*" "*just do what you're told,*" or "*we don't have time for this stuff*," sustained champion engagement will be difficult regardless of your programme design.

In these cultures, you may need a different approach. Rather than building a large champions network with many volunteers, focus on a small number of highly committed individuals, provide them with substantial support, and demonstrate the value of their contributions. As that value becomes visible, cultural resistance may decrease.

Alternatively, consider whether champions need more formal recognition of security responsibilities in their role definitions and performance expectations. If the culture doesn't value voluntary contribution, perhaps security champion work needs to be an explicit part of certain roles rather than a voluntary addition.

The Culture Check

Before launching or when struggling with engagement, assess your culture honestly. How does your organisation typically respond to volunteer initiatives? What happens to people who take on extra responsibilities? Are they celebrated or viewed suspiciously? If cultural signals are negative, adjust your approach. You might need a stronger executive mandate, more formal role definitions, or an explicit connection to career progression. Don't assume a volunteer model will work simply because it works elsewhere.

The Long-Term View

Security Champions programmes deliver their full value over years, not months. Initial enthusiasm creates momentum, but sustained discipline builds capability and culture change.

The champions who've been engaged for two years understand security deeply, influence broadly, and proactively prevent issues. Teams that have had effective champions for multiple years develop a security mindset as the default. The organisation that has maintained a champions programme for several years has materially improved its security posture through distributed expertise.

None of that happens without sustained engagement. And sustained engagement requires constant attention to development, value creation, recognition, and support.

You're not building a programme that launches successfully. You're building one that sustains and compounds its impact over time. That requires different thinking, different practices, and different measures of success.

The next chapter explores how to demonstrate long-term value through measurement and reporting that maintains executive support and programme investment even as initial novelty fades.

PART III: MAKING IT WORK

Chapter 6: Measuring Success and Demonstrating Value

Six months into his Security Champions programme, David faced a problem. His champions were engaged, they were developing capability, and anecdotally, he knew they were having an impact. But when his executive sponsor asked *"Is this working?"*, David struggled to provide a compelling answer beyond "I think so."

He had metrics. Lots of them. Number of champions recruited, training sessions completed, vulnerabilities identified, and hours invested. But none of these answered the fundamental question his sponsor was really asking: *"Is this programme delivering enough value to justify continued investment?"*

This is the measurement challenge every programme leader faces. You need to demonstrate value convincingly enough to maintain executive support and secure resources. But the value champions create is often diffuse, preventative, and difficult to quantify precisely. You can't simply count widgets produced when the primary value is problems prevented.

This chapter explores how to measure what matters, demonstrate value effectively, and build the business case that sustains programme investment over time. Not through elaborate measurement frameworks that require dedicated analysts to maintain, but through practical approaches that busy programme leaders can implement whilst running their programmes.

The Measurement Trap

Before diving into what to measure, let's address what not to measure. Many programmes fall into measurement traps that create work without creating insight.

Vanity Metrics That Don't Matter

The easiest things to measure are often the least meaningful. Number of champions recruited. Training completion rates. Slack channel message counts. Meeting attendance percentages. These metrics are simple to track, but they don't tell you whether your programme is effective.

A programme with 50 recruited champions might be less effective than one with 20 if most of those 50 are disengaged. Training completion rates tell you who finished courses, not whether they're

applying what they learned. High message counts might indicate confusion rather than collaboration.

These vanity metrics serve one useful purpose: tracking basic health indicators. If meeting attendance drops sharply, that signals declining engagement. If training completion is very low, that suggests your training approach isn't working. But don't confuse health indicators with value indicators.

Marcus ran a programme that reported impressive activity metrics to leadership: 45 champions, 200 security reviews completed, 1,500 community messages. His sponsor was pleased until an audit revealed that their security posture hadn't improved meaningfully. The champions were active but not effective. They were conducting reviews but not catching issues. They were messaging but not learning. Activity without impact.

The Measurement Paradox

The things that are easiest to measure are often the least important. The most important things are often the hardest to measure. The number of vulnerabilities prevented is more valuable than the number of vulnerabilities found, but you can only count what you found. A cultural shift toward security thinking matters more than the number of training hours completed, but culture is harder to quantify. Don't let measurement ease drive what you measure. Start with what matters, then figure out how to measure it well enough.

Precision Versus Direction

You don't need precise measurements. You need measurements good enough to show whether things are getting better, staying the same, or getting worse. Direction matters more than exact numbers.

If security incidents in teams with champions are declining whilst incidents in teams without champions are steady, that's compelling evidence of value, even if you can't prove the exact percentage improvement attributable to champions versus other factors.

If champions are handling more complex security decisions independently over time, that demonstrates capability development, even if you can't quantify their exact expertise level with numerical precision.

If teams are incorporating security earlier in their processes, that indicates culture change, even if you can't measure "security culture" on an absolute scale.

Sarah, a programme leader at a healthcare organisation, learned this through experience: *"I spent months trying to develop a rigorous ROI model that calculated the precise financial value of prevented incidents. It was impossible because we couldn't know what would have happened without champions. I shifted to showing clear trends: incidents declining in champion teams, security issues caught earlier*

in development, and teams asking security questions proactively. Less precise but more convincing because it showed direction clearly."

What Actually Matters

Effective measurement focuses on three fundamental questions: Are champions developing capability? Are they having an impact? Is the programme sustainable? Let's explore how to address each.

Measuring Capability Development

Champions must develop security capabilities to be effective. Tracking this development demonstrates that your training and support approaches work whilst increasing their value to champions.

The Good Enough Measurement Principle

For each metric you're considering, ask: "Will this measurement be good enough to inform decisions and demonstrate value?" If yes, implement it even if it's imperfect. If no, find a better metric or accept you can't measure that dimension precisely. Perfect measurement is the enemy of useful measurement. Better to have directionally accurate insights you can act on than precisely accurate measurements of things that don't matter.

Self-assessment surveys provide baseline capability measurement. Ask champions quarterly to rate their confidence in key areas: identifying common vulnerabilities, conducting code reviews with security lens, making risk-based security decisions, and explaining security concerns to stakeholders. Track how these confidence levels change over time.

This isn't an objective measurement of capability, but it captures champions' perception of their own development. Champions who feel more capable are more likely to engage and take on challenges. Improving confidence is valuable even if you can't verify exact capability levels.

Rachel's programme does this simply: *"Every quarter, champions rate themselves on ten key capabilities using a five-point scale. We track the average rating for each capability over time. In the first year, we saw average ratings increase from 2.3 to 3.8. That's meaningful progress. We don't need to know their exact capability level to see they're developing."*

Behavioural indicators show capability through action rather than self-report. Track what champions are doing that they couldn't or wouldn't do previously.

Are champions who initially escalated all security questions now handling routine issues independently? That demonstrates growing technical capability and confidence.

Are champions providing input earlier in development cycles? That indicates they understand how to identify security concerns in design phases rather than just reacting to completed code.

Are champions teaching others? A champion who runs a secure coding workshop for their team demonstrates capabilities well beyond basic security awareness.

James tracks behavioural progression systematically: "We record the types of activities each champion engages in monthly. New champions mainly ask questions and attend training. After three months, they're answering routine questions from teammates. After six months, they're conducting security reviews and influencing design decisions. After a year, they're training others and working on strategic improvements. This progression shows capability development clearly."

Peer and manager feedback provides external validation. Quarterly check-ins with champions' teammates and managers, asking simple questions: *"Is [Champion] contributing more effectively to security than six months ago?" "What security capabilities has*

[Champion] developed recently?" "How valuable is [Champion's] security input to the team?"

This feedback validates whether capability development is translating into practical contribution. A champion who rates themselves highly but whose team sees no improvement probably has overconfident self-assessment rather than genuine capability.

Measuring Security Impact

Capability development matters because it enables impact. Champions should materially improve their teams' security posture. Measuring this impact demonstrates the programme's core value.

Incident and vulnerability trends provide hard data about security outcomes. Compare teams with champions to teams without champions (or the same teams before and after getting champions).

Are security incidents declining in champion teams? Are vulnerabilities found in production decreasing? Are security issues being caught earlier in development? Are teams requesting fewer last-minute security exemptions because they're building security in from the start?

These metrics have limitations. Incident rates can fluctuate for reasons unrelated to champions. Different teams face different

security risks. Correlation doesn't prove causation. But clear trends across multiple teams over sustained periods provide compelling evidence.

Emma runs a programme at a financial services firm with rigorous measurement: *"We track security issues by severity and discovery phase for all teams. Teams with champions show 40% fewer high-severity issues reaching production compared to teams without champions, and they catch issues an average of two sprints earlier. We can't prove champions caused all that improvement, but the correlation is strong enough to be convincing."*

Security process improvements indicate the influence of champions on how teams work. Measuring these improvements shows champions aren't just finding individual issues but improving underlying practices.

Are more teams conducting threat modelling for new features? Are security reviews happening earlier in the development cycle? Are teams adopting security tooling or practices that champions advocate? Are security requirements being included in sprint planning rather than discovered during security reviews?

Track adoption of security practices across teams. Champions should accelerate adoption in their teams compared to teams without champions.

Early issue identification demonstrates preventative value. One of the champions' most important contributions is catching security problems when they're cheap to fix rather than expensive to remediate.

Track where in the development lifecycle security issues are discovered. Issues found during design cost little to address. Issues found in code review cost more. Issues found in production cost dramatically more. Champions should shift the distribution toward earlier discovery.

Michael's programme measures this explicitly: *"We categorise every security issue by where it was discovered: design phase, development, code review, testing, production. Teams with champions find 65% of issues during design or development, compared with 30% for teams without champions. That early detection saves massive remediation costs."*

The Prevented Incident Problem

The most valuable thing champions do is prevent security incidents from occurring in the first place. But you can't easily measure something that didn't happen. A champion who spots a critical design flaw and prevents a potential breach created enormous value, but there's no incident to count. This is why tracking early issue identification and process improvements matters.

Measuring Programme Sustainability

Even effective programmes fail if they're not sustainable. Measuring sustainability helps you identify and address issues before they undermine programme success.

Champion engagement and retention indicate whether champions find the programme valuable enough to maintain participation.

Track active engagement rates. What percentage of champions are participating in community discussions, attending meetings, and completing development activities? Declining participation signals sustainability problems.

Track retention rates. What percentage of champions remain actively engaged after six months? After twelve months? High attrition suggests champions aren't getting sufficient value or support.

Track reasons for departure when champions leave. Departures due to role changes are inevitable. Departures due to feeling overwhelmed or unsupported indicate problems with programme design.

Time investment tracking reveals whether your programme asks too much or provides too little support.

Survey champions quarterly about the actual time spent on champion activities. Compare this to your stated expectations. If champions consistently spend significantly more time than expected, your role scope may be unrealistic. If they spend less, they may not be fully engaged, or your expectations may be too low.

Track where champions spend time. If most time goes to low-value activities like meetings and administrative tasks rather than high-impact security work, your programme design needs adjustment.

Stakeholder satisfaction measures whether the people champions value their contribution.

Survey teams, managers, and the security team about the effectiveness and value of the champion. Do teams find their champions helpful? Do managers see security improvement? Does the security team view champions as effective collaborators?

Declining satisfaction suggests champions may be losing effectiveness even if activity metrics remain strong.

Louise tracks stakeholder satisfaction systematically: *"We send a quarterly pulse survey to teams with champions, asking three questions: How valuable is your champion's contribution? How has your team's security posture changed? What could improve? The first year showed satisfaction scores increasing from 3.2 to 4.1 out of 5.*

That validated our programme was delivering value to the teams we exist to serve."

Building Your Measurement Framework

You don't need dozens of metrics. You need the right metrics measured consistently and reported clearly. Here's how to build a practical measurement framework.

Selecting Core Metrics

Choose a small set of core metrics that provide insight into the three critical dimensions: capability, impact, and sustainability. A total of five to ten metrics is typically sufficient.

Your core metrics should be:

- **Meaningful**: They measure things that matter to programme success
- **Actionable**: Results inform decisions about programme improvements
- **Collectable**: You can gather the data without heroic effort
- **Understandable**: Stakeholders can interpret what the metrics mean without extensive explanation

Start with a candidate list of possible metrics, then ruthlessly prioritise. Which metrics provide the most insight with the least effort

to collect? Which metrics will be most convincing to your executive sponsor? Which metrics help you identify and address problems early?

Test your proposed metrics by asking: *"If this metric shows a negative trend, what would I do differently?" If you can't answer that question, the metric probably isn't useful.*

Establishing Baselines and Targets

Measurements only become meaningful when you have baselines and targets for comparison.

Establish baselines before launching your programme or as early as possible after launch. What's the current state of key metrics? How many security incidents occur in teams that will get champions? What's the current distribution of when security issues are discovered? How confident are prospective champions in their security capabilities?

Without baselines, you can't demonstrate improvement. A champion team with five security incidents this quarter may sound concerning, but it's worth noting that they had twelve incidents in the quarter before they had a champion.

Set realistic targets based on benchmarks from other organisations or reasonable expectations given your context. Don't expect

perfection. Demonstrating 30-40% improvement is often more credible than claiming 80-90% improvement.

Also set targets for different timeframes. What do you expect to achieve in the first six months? The first year? The second year? Early targets should be achievable with modest effort. Later targets can be more ambitious as champions develop capability and the programme matures.

David's approach*: "We established baselines for five key metrics before recruiting our first champions. We set conservative six-month targets: a 20% reduction in late-stage security issues, a champion confidence average of 3.0 out of 5, and 80% champion retention. We actually achieved 35% reduction, 3.4 confidence, and 85% retention. Beating conservative targets was more credible than setting aggressive targets and missing them."*

Creating Collection Processes

Measurement only works if you actually collect data consistently. Design collection processes that are sustainable, given your available time and resources.

Automated collection where possible. If you can pull incident data from existing systems rather than manually tracking it, do so. If

champions log security reviews in your ticketing system, extract that data rather than asking champions to report separately.

Minimal manual reporting where automation isn't possible. Simple monthly or quarterly surveys that take champions five minutes to complete. Brief quarterly check-ins with managers that capture key feedback without demanding extensive time.

Regular collection cadence so measurement becomes routine rather than a special effort. Monthly collection of some metrics, quarterly collection of others, and annual collection of deeper assessments. Regular cadence makes collection habitual and provides timely insights.

Document your collection processes clearly so anyone could execute them if you're unavailable. .

The Measurement Burden Trap

A technology company built an elaborate measurement framework that collected 25 metrics monthly. The programme leader spent 15-20 hours per month on measurement, leaving less time to support champions. Worse, the extensive reporting created noise that obscured important signals. They simplified to eight core metrics, automated half of them, and reduced measurement time to four hours monthly. Measurement quality improved because they could analyse and act on fewer, better metrics.

Demonstrating Value to Different Stakeholders

Different stakeholders care about different aspects of programme value. Effective communication tailors your message to each audience.

Executive Sponsors

Executives care primarily about business outcomes and strategic value. They want to know the programme is delivering return on investment, enabling business objectives, and managing risk appropriately.

Frame impact in business terms. Don't just report that champions identified 47 vulnerabilities. Explain that champions prevented security issues that would have delayed product launches, created compliance violations, or exposed customer data. Connect security outcomes to business impact.

Show trends over time. Executives want to see whether things are improving. Use simple trend charts that show key metrics over time, with clear direction indicators. Declining incident rates in champion teams. Increasing security issue identification in early development phases. Growing champion capability and confidence.

Compare to alternatives. What would the business outcomes be without the champions programme? Higher incident rates, more expensive late-stage remediation, and delayed product launches due to security issues discovered at the last minute. Champions create value partly by avoiding these costs.

Keep it concise. Executives are busy. A one-page executive summary with three to five key metrics and clear conclusions is more effective than a detailed ten-page report that they won't read.

Rachel presents to her executive sponsor quarterly: *"I prepare a single-slide dashboard showing five metrics with trend arrows and one-sentence interpretations. Champion teams: 42% fewer production security issues than baseline. Issues found: 58% during design/development versus 31% baseline. Champion capability: average 3.9/5.0 versus 2.4/5.0 at start. Retention: 87% after 12 months. Value delivered: estimated £340,000 in prevented incident costs. My sponsor can digest this in 60 seconds and ask questions about anything that concerns them."*

The One-Metric Rule for Executives

If you could only show your executive sponsor one metric, which would be most convincing? That's your north star metric. For some programmes, it's about reducing incidents in champion teams. For

others, it's the percentage of security issues caught in early development phases. For others, it's champion engagement and satisfaction scores. Lead with your north star metric in every executive communication. Other metrics provide context, but your north star metric drives the value narrative.

Security Team

The security team cares about whether champions are effective security collaborators who reduce the team's workload and improve the security posture.

Demonstrate capability development. Show that champions are developing genuine security expertise, not merely repeating security team guidance without understanding it. Share examples of sophisticated security analyses or decisions champions have made. Highlight areas where champions now operate independently rather than requiring support from the security team.

Show workload impact. Are champions reducing the security team's burden? Fewer escalations of routine issues. Faster security reviews because champions prepare their teams well. More effective collaboration because champions translate security requirements into their teams' context. Quantify this impact where possible.

Share champion contributions. The security team needs to see specific examples of valuable work champions are doing. Vulnerabilities that the security team might have missed. Process improvement champions drove enhancements in security. Teams' champions are influenced to adopt better practices.

Acknowledge challenges honestly. The security team knows the programme reality. Don't oversell champion effectiveness. Share what's working and what isn't. Discuss how the security team can better support champions. This builds credibility and partnership.

Michael's approach with the security team*: "I send a monthly newsletter highlighting specific champion contributions: 'Champion Alex identified a race condition in the payment processing flow that our standard security review would have missed.' 'Champion Sarah got her team to adopt automated security testing, reducing their security review time from three days to eight hours.' I also share challenges: 'Three champions need additional support on threat modelling' or 'Infrastructure champions struggling with cloud security concepts.' The security team sees both the value and the reality."*

Champions' Managers

Champions' managers care about whether championing benefits their employees' development and doesn't impair team performance.

Show professional development. Highlight skills champions are developing that benefit them professionally: security expertise, influence skills, cross-functional collaboration, and technical leadership. Connect championing with the capabilities managers value.

Demonstrate team benefit. Managers want to know their team's security is improving without creating excessive overhead. Show that having a champion reduces security friction, catches issues early, and accelerates development by preventing late-stage security problems.

Acknowledge time investment transparently. Don't hide the time champions spend on programme activities. Show it's reasonable and valuable. Champions who spend 5-6 hours monthly on security activities that prevent multi-day remediation are a good investment.

Recognise individual champions. When champions do excellent work, tell their managers. Managers appreciate knowing their team

members are contributing beyond their immediate team and developing valuable expertise.

Louise manages this relationship carefully: *"When I meet with champions' managers, I lead with what their employee is learning and contributing. 'Sarah developed threat modelling expertise that helped her team avoid a major security redesign that would have delayed their launch by three weeks.' 'James is now teaching secure coding practices to new hires, which is accelerating their team's onboarding.' Managers see championing as professional development that benefits everyone."*

The Manager Resistance Problem

Some managers view champions as a distraction from "real work" or resent the time commitment. This resistance undermines champion engagement and programme sustainability. Address it by demonstrating tangible team benefits: faster security reviews, fewer late-stage surprises, improved security posture. Also work with programme sponsors to ensure senior leadership communicates that security championing is a valued contribution, not optional volunteer work. Manager attitudes shift when they see their peers' champions delivering clear value.

Champions Themselves

Champions need to see that their efforts matter and that they're developing valuable capabilities. Internal reporting to champions serves different purposes than external reporting to stakeholders.

Celebrate collective impact. Share what the champion community achieved collectively. Total security issues identified across all champions. Number of teams adopting improved security practices through champion influence. Overall improvement in organisational security posture. Champions should see they're part of something meaningful.

Recognise individual contributions. Publicly acknowledge specific champions who made notable contributions. This provides recognition whilst showing all champions what excellent championing looks like.

Show capability progression. Help champions see their own development through capability assessments and progression tracking. Champions who see themselves improving are motivated to continue developing.

Gather and share champion stories. Create spaces for champions to share successes and learnings. These stories inspire other champions whilst creating community cohesion.

Alex runs a monthly "champion wins" discussion: *"Each month, champions share recent successes in our community channel. Someone caught a vulnerability that would have been catastrophic. Someone convinced their team to adopt security testing. Someone helped another team resolve a complex security challenge. These stories remind everyone that championing matters and show practical examples of effective championing."*

The Recognition Rhythm

Establish a regular rhythm for recognising champion contributions. Monthly highlights in the champion community. Quarterly awards or call-outs in programme updates. Annual recognition for sustained contribution. Regular recognition maintains motivation whilst helping champions see the impact they have, both collectively and individually. Don't save all recognition for annual reviews; frequent small recognition sustains engagement better than infrequent large recognition.

Making the Business Case

Beyond regular measurement and reporting, you periodically need to make formal business cases for programme investment, whether for initial funding, expansion, or continuation.

Quantifying Value When Possible

Some programme values can be quantified in financial terms. Not with perfect precision, but well enough to be credible.

Prevented incident costs provide tangible financial value. If champions prevented a data breach, what would that breach have cost in regulatory fines, remediation, customer notification, and reputational damage? If champions caught a vulnerability before production, what would it have cost to remediate in production versus development?

Use conservative estimates based on industry benchmarks or your organisation's past incidents. Preventing one major incident might justify your entire programme budget for a year.

Accelerated delivery value comes from avoiding security-related delays. If champions help teams build security in from the start rather than discovering issues at the end, projects complete faster. Calculate the value of that time saving.

Reducing the security team's burden has financial implications. If champions handle work that would otherwise require the security team's time, you're effectively increasing the security team's capacity without hiring additional staff. Calculate what that capacity is worth.

David builds this case annually: *"We track high-severity security issues prevented by champions catching problems in design or development. Using our standard incident cost model, those preventions averaged £125,000 per incident. Last year, champions prevented 11 such incidents, representing £1.4 million in avoided costs. Our programme costs £180,000 annually. Even if our estimates are off by 50%, we're delivering substantial return on investment."*

Articulating Qualitative Value

Not all value can be quantified, but qualitative value still matters and can be articulated compellingly.

Cultural transformation toward security thinking. Champions create environments where security is a normal consideration rather than an afterthought. Teams ask *"Is this secure?"* as naturally as *"Is this functional?"* That cultural shift delivers long-term value that's hard to quantify but easy to observe.

Capability building across the organisation. Every champion becomes more security-capable, and their teams learn from them. You're building distributed security expertise that makes your organisation more resilient and adaptable.

Risk reduction that doesn't show up in incident metrics. Better security practices reduce the likelihood of incidents that haven't

happened yet. That risk reduction is valuable even if you never experience the incidents you prevented.

Competitive advantage in markets where security matters. Organisations with a strong security posture win customer trust, meet regulatory requirements more easily, and can pursue opportunities others can't because of security constraints.

Sarah makes this case alongside quantitative metrics: *"Beyond prevented incident costs, our champions programme fundamentally changed how our engineering teams think about security. Design discussions now include security considerations by default. Teams proactively reach out with security questions rather than avoiding security until reviews. New engineers learn secure development*

The Story and Numbers Approach

The most compelling business cases combine quantitative evidence with qualitative stories. Lead with a concrete example: "Our champion in the payments team identified a critical authorisation flaw during design review that would have exposed £2.3 million in transaction data if it reached production." Then provide the numbers: "Across all champions, we prevented 23 high-severity issues with estimated costs of £340,000 in remediation and potential incident response." Then articulate the broader value: "More importantly, teams now design with security in mind rather than bolting it on afterwards." Numbers prove value. Stories make it vivid and memorable.

practices from day one because champions integrate security into onboarding. This cultural shift delivers compounding value that incident metrics alone don't capture."

Using Measurement to Improve

Measurement's ultimate purpose isn't reporting but improvement. Your metrics should inform programme enhancements and identify what needs to change.

Identifying What's Working

Look for positive patterns in your metrics. Which champion activities correlate most strongly with security improvements? Which development approaches produce the greatest capability gains? Which engagement mechanisms sustain participation most effectively?

Double down on what's working. If pairing new champions with experienced champions accelerates capability development more than formal training, invest more in pairing. If champions in certain roles have an outsized impact, focus recruitment on similar roles.

Emma uses measurement to guide programme evolution: *"We tracked which types of champion activities had the most security impact. Turns out champion involvement in architecture and design*

reviews prevented far more issues than champion involvement in later-stage code reviews. We shifted our programme's emphasis to ensure champions engage early in the design process. Impact increased measurably."

Diagnosing Problems Early

Watch for negative trends or warning signs in your metrics. Declining engagement. Capability development is plateauing. Stakeholder satisfaction is dropping. These signals indicate problems that need to be addressed.

Investigate underlying causes. If engagement is declining, why? Are expectations unrealistic? Is the value unclear? Are champions feeling unsupported? Understanding root causes enables targeted solutions.

Act on insights promptly. If you identify problems in metrics but don't adjust the programme, champions lose confidence that their feedback matters and that programme leadership is responsive.

Michael caught a problem through measurement: *"Our retention metrics showed champions typically left around the nine-month mark. We found that experienced champions felt they'd stopped developing and were repeating the same activities. We introduced advanced development opportunities and strategic project*

involvement for experienced champions. Retention improved significantly."

Testing Hypotheses

Use measurement to test programme improvements. If you believe a change will improve outcomes, measure before and after to validate your hypothesis.

You're considering switching from monthly champion meetings to quarterly workshops. Measure engagement and satisfaction before the change and three months after. Did the change improve or harm those metrics?

You think pairing champions with similar specialities will accelerate capability development. Implement pairing for half your champions and track capability development for paired versus unpaired champions. Does the data support your hypothesis?

This experimental mindset prevents you from changing things based on assumptions that turn out to be wrong, whilst validating successful innovations you can scale.

The Measurement Feedback Loop

The most successful programmes create a feedback loop: measure outcomes, identify opportunities for improvement, implement changes, measure again to validate impact, and iterate. This continuous improvement approach keeps programmes evolving and getting better over time. Programmes that measure but don't act on insights stagnate. Programmes that change without measuring can't tell whether changes helped or hurt. The combination of measurement and action drives sustained programme improvement.

Common Measurement Mistakes

Even well-intentioned measurement efforts can go wrong. Watch for these common mistakes.

Measuring Too Much

The temptation is to measure everything that might be interesting. This creates overwhelming amounts of data that nobody has time to analyse or act on. You spend more time gathering and reporting metrics than using them to improve the programme.

Focus on the vital few metrics that provide the most insight. Add metrics only when you have clear reasons and the capacity to use

them. Remove metrics that aren't informing decisions or demonstrating value.

Measuring Too Little

The opposite mistake is measuring so little that you can't demonstrate value convincingly or identify problems early. Relying only on anecdotal evidence or champion satisfaction surveys doesn't build compelling business cases.

Ensure you're measuring all three critical dimensions: capability development, security impact, and programme sustainability. If any dimension is unmeasured, you have blind spots that could hide serious problems.

Gaming the Metrics

When you measure activities, people optimise for those metrics sometimes at the expense of actual outcomes. Champions might focus on identifying many low-severity vulnerabilities because those are easier to find and count, while missing fewer high-severity issues that matter more.

Mitigate gaming by measuring outcomes and impact rather than just activities. Measure security posture improvements, not just the number of security reviews conducted. Measure capability development, not just training completion.

Also, use multiple metrics so gaming any single metric doesn't create a misleading overall picture.

Changing Metrics Frequently

Consistency matters more than perfection in measurement. If you change what you're measuring every quarter, you can't track trends or demonstrate improvement over time.

Select metrics thoughtfully, then stick with them long enough to see meaningful trends. Adjust metrics when you have good reasons, but not simply because you're unsure or want to try something different.

Building Credibility Through Measurement

Ultimately, measurement serves to build and maintain credibility with stakeholders. Your measurement approach should demonstrate rigour without overreaching, honesty without underselling, and insight without overwhelming.

Be Honest About Limitations

Acknowledge what you can and can't measure precisely. Don't claim exact return on investment when you're actually making reasonable estimates. Don't pretend correlation proves causation when other factors might be contributing.

This honesty builds credibility. Stakeholders trust leaders who acknowledge uncertainty more than those who claim unjustified precision.

Rachel's approach*: "When I present prevented incident costs, I explicitly say 'These are conservative estimates based on industry benchmarks. The actual costs could be higher or lower, but this gives us a reasonable sense of value magnitude.' Stakeholders appreciate that I'm not pretending to have perfect data whilst still giving them useful information for decision-making."*

Show Your Work

Explain how you calculated metrics and what assumptions you made. This transparency helps stakeholders understand and trust your numbers.

If you're calculating prevented incident costs, show the assumptions: the average cost of similar incidents, the severity distribution, the likelihood that the issue would have reached production, and the remediation costs avoided. Stakeholders can assess whether assumptions are reasonable.

Track Long-Term Trends

Short-term metrics fluctuate. One quarter might show worse security outcomes for reasons unrelated to your programme. Long-term trends are more meaningful and harder to explain away through special circumstances.

Show metrics over time, not just point-in-time snapshots. A year-over-year trend showing sustained improvement is more convincing than a single quarter's results.

Connect to Organisational Priorities

Frame your metrics in terms that matter to stakeholders. If your organisation is focused on rapid product delivery, emphasise how champions accelerate delivery by preventing late-stage security delays. If regulatory compliance is a priority, highlight how champions improve compliance posture. If customer trust matters, show how champions strengthen security that protects customer data.

Your programme delivers value. Make sure stakeholders can see how that value connects to what they care about most.

Sustaining the Measurement Practice

Measurement must be sustainable over the long term, or it won't be consistent enough to be useful.

Build It Into Your Rhythm

Make measurement part of your regular programme rhythm rather than a separate effort you squeeze in. Block time monthly for basic metric collection. Schedule quarterly deep analysis sessions. Plan annual comprehensive reviews.

When measurement is calendared and routine, it happens. When it's something you do in your free time, it gets deferred during busy periods.

Automate What You Can

Invest time upfront to automate metric collection where possible. Scripts that pull data from ticketing systems. Automated surveys that collect and aggregate responses. Dashboard tools that visualise metrics automatically.

Initial automation setup takes time but pays dividends through reduced ongoing effort and more consistent data collection.

Make It Collaborative

Involve champions and the security team in measurement. They can help collect data, provide context for interpreting metrics, and benefit from insights you gain.

Champions might track their own activities in a simple shared spreadsheet. Security team members might provide data about champions' contributions to security reviews. This distributed collection reduces the burden whilst creating shared investment in measurement.

Keep It Simple

Resist the urge to make measurement increasingly sophisticated unless sophistication adds value. A simple spreadsheet tracking core metrics over time often serves better than an elaborate business intelligence dashboard that requires dedicated maintenance.

Sophistication should serve clarity and insight, not impress stakeholders with complexity.

The Continuous Improvement Mindset

Measurement enables continuous improvement, but doesn't guarantee it. You must create habits and practices that translate measurement insights into programme enhancements.

Review metrics regularly with genuine curiosity about what they're telling you. When metrics show positive trends, investigate why to reinforce what's working. When metrics reveal concerning patterns, dig into the root causes to address them.

Share insights with champions and other stakeholders. Measurement creates a shared understanding of programme state and builds collective commitment to improvement.

Test changes on a small scale before implementing broadly. If you think a programme modification will improve outcomes, try it with a

The Measurement MVP

Start with a minimal viable measurement practice: three to five core metrics, simple collection processes, and basic trend analysis. Get this working sustainably before expanding. Many programmes fail at measurement because they start too ambitiously, can't sustain the effort, and abandon measurement entirely. Better to start simple and expand gradually than to start elaborate and collapse under the burden.

subset of champions first and measure results before rolling it out universally.

Document what you learn from measurement so insights accumulate over time rather than being rediscovered repeatedly.

David reflects on his measurement journey: *"Initially, I saw measurement as something I did to report to stakeholders. Now I see how I can improve the programme. Metrics tell me what's working and what isn't, what champions need, and where to invest effort. Measurement transformed from a burden into a tool that makes me more effective as a programme leader."*

That transformation represents the ultimate value of measurement. Not just demonstrating value to others, but creating the insights that let you deliver more value through continuous programme improvement.

The next chapter explores the practical wisdom that complements formal measurement: lessons learned from successful programmes, mistakes others made that you can avoid, and non-obvious insights that separate exceptional programmes from merely adequate ones.

Chapter 7: Practical Wisdom for Success

If you've read this far, you understand the theory behind Security Champions programmes. You know how to secure executive support, design your network, develop champions, and measure value. But theory and practice diverge in predictable ways.

This chapter contains the wisdom that doesn't fit neatly into structured frameworks. The lessons programme leaders learn through experience, often the hard way. The non-obvious insights that separate programmes that thrive from those that merely survive. The practical advice that helps you navigate the messy reality of building something new in an organisation that's already busy.

These aren't sequential steps or comprehensive frameworks. They're hard-won insights from programme leaders who've made mistakes so you don't have to, discovered shortcuts that save months of effort, and learned when to bend rules and when to hold firm.

Starting Strong

How you launch your programme shapes everything that follows. Get the start right, and you build momentum. Get it wrong, and you spend months recovering.

Don't Wait for Perfect

The biggest mistake new programme leaders make is waiting until everything is perfect before launching. The perfect training curriculum, the perfect champion recruitment process, the perfect measurement framework. These don't exist.

Launch when you're ready enough, not when you're perfect. Ready enough means you have executive support, you've identified your first champions, and you have a basic plan for the first three months. Everything else can be refined as you go.

Sophie delayed her programme launch by five months whilst developing comprehensive documentation, detailed role descriptions, and elaborate training materials. When she finally launched, much of what she'd created needed immediate revision because it didn't match reality. "I should have launched three months earlier with 70% of what I eventually created, then refined based on actual experience rather than theoretical planning."

Early champions are remarkably forgiving of imperfection if you're honest about learning together. They'll tolerate rough processes and incomplete resources if they see you're responsive to feedback and genuinely trying to support them.

The Three-Month Plan

Rather than planning your entire programme in detail upfront, plan intensively for the first three months and broadly for months 4-12. Focus your energy on getting champions started well, building early relationships, and creating initial value. Once you have three months of experience, you'll plan subsequent phases far more effectively because you understand your actual context rather than your imagined one.

Start with Volunteers

Your first champions should be volunteers who are genuinely interested, not conscripts who've been voluntold by their managers. Voluntary participation signals intrinsic motivation that sustains engagement when challenges arise.

This means your initial coverage will be incomplete. You won't have champions in every team or domain. That's fine. Better to start with ten engaged volunteers than thirty half-hearted conscripts.

Those initial volunteers become your foundation. They help you refine programme elements, demonstrate value that attracts subsequent champions, and provide peer support as you expand. Your second cohort of champions joins a programme with proven value rather than an experiment.

James ran his initial recruitment broadly, accepting everyone who volunteered regardless of their motivation. *"Some people volunteered because they cared about security. Others volunteered because they thought it would look good on their CV, or their manager pressured them. The first group thrived. The second group quietly disengaged. If I'd screened more carefully initially, I would have saved significant wasted effort supporting people who were never really committed."*

The Pressure Volunteer Problem

Sometimes managers pressure team members to volunteer as champions even when those individuals aren't genuinely interested. These "pressure volunteers" rarely engage meaningfully but feel they can't decline. Screen for genuine interest during recruitment conversations. Ask why they're interested in championing and what they hope to gain. If answers are vague or focus solely on external pressure, help them decline gracefully rather than accept reluctant participants who'll disengage anyway.

Invest Heavily in Onboarding

The first month determines whether new champions engage or drift away. Invest disproportionate energy in onboarding your first cohort and each subsequent cohort.

Effective onboarding includes:

- ✓ Clear explanation of what champions do and don't do. Realistic expectations about time commitment and responsibilities. Explicit permission to ask questions and make mistakes whilst learning.
- ✓ Introduction to the champion community and key security team members. Champions need to know who to ask for help and feel part of something bigger than themselves.
- ✓ Quick wins that build confidence. New champions should achieve something meaningful in their first two weeks, even if it's small. Catching one security issue or successfully answering a teammate's question builds confidence, motivating continued engagement.
- ✓ Connection to why this matters. Remind champions that their work prevents real problems, protects real users, and makes their organisation more secure. Purpose sustains motivation during challenging periods.

Rachel runs an intensive onboarding: *"New champions attend a half-day session where they meet the security team, learn basic security concepts for our environment, and get introduced to current champions. We pair each new champion with an experienced champion buddy for their first two months. We give them a specific task to complete in week one that guarantees early success. This investment pays off through much higher sustained engagement."*

Building Relationships That Matter

Programmes succeed through relationships more than through processes. The connections between champions, between champions and the security team, and between champions and their leaders determine programme health.

The Security Team Partnership

The relationship between programme leadership and the security team makes or breaks programmes. You need the security team to respect champions as valuable collaborators rather than viewing them as amateurs who create more work.

Build this partnership deliberately. Involve the security team in programme design. Ask for their input on champion training, their guidance on escalation processes, and their feedback on

programme effectiveness. This involvement creates ownership rather than tolerance.

Make champions' contributions visible to the security team. When champions identify significant issues, tell the security team who caught them and how. When champions help their teams implement security improvements, share those successes. The security team needs to see concrete evidence of champion value.

Acknowledge security team concerns honestly. If champions are escalating issues inappropriately or providing incorrect guidance, address those problems rather than automatically defending champions. The security team will trust you more if they see you holding champions accountable for quality.

Michael works intentionally on this relationship*: "I meet with security team leads monthly to discuss how champions are contributing and*

The Security Team Advisory Group

Establish a small advisory group comprising security team members to provide ongoing input on programme direction. Meet quarterly to review what is effective, identify areas needing adjustment, and consider how the programme can better support security objectives. This structure ensures ongoing security team participation while preventing programme capture, where security team preferences overshadow champion and business needs..

where they need development. When the security team raises concerns about specific champions, I address them directly rather than getting defensive. When champions do excellent work, I make sure the security team knows. This partnership approach means the security team views champions as extensions of their capability rather than as problems they must manage."

Champion-to-Champion Connections

The strongest programmes have champions who genuinely know and support each other. These relationships enable peer learning, provide motivation during difficult periods, and create a community that sustains engagement.

You can't force authentic relationships, but you can create conditions that allow them to develop naturally.

Facilitate introductions between champions who share interests or face similar challenges. Connect the champion struggling with threat modelling to the champion who's mastered it. Introduce champions working on similar technical stacks who can share security patterns.

Create spaces for informal interaction beyond work-focused meetings. Social time before or after champion sessions. Dedicated

channels for non-work discussion. Optional social events where champions can connect personally.

Celebrate collective achievements that reinforce champions' identity as part of something meaningful. When the champion community collectively achieves something significant, acknowledge it publicly and remind champions they're part of that success.

Emma deliberately builds champion connections: *"We start every quarterly champion session with 30 minutes of informal connection time with refreshments. We have random coffee-pairing where we match champions who haven't interacted recently for virtual coffee chats. We maintain a 'random' channel where champions share interesting non-work things. These might seem peripheral to security, but they build relationships that make champions willing to help each other with security challenges."*

Connecting Champions to Leadership

Champions need visibility to organisational leadership, and leadership needs to see champion contributions. Without this connection, champions feel undervalued, and leadership may question programme value.

Create structured opportunities for champion-leadership interaction. Champions presenting at architecture reviews. Champions participating in security strategy discussions. Champions sharing their work at engineering all-hands meetings. These interactions demonstrate champion expertise whilst making their contributions visible.

Ensure champions' managers understand and value their security work. When champions do excellent work, tell their managers. When champions develop new capabilities, ensure their managers know. Champions whose managers value their security contribution are far more likely to sustain engagement.

Louise manages this carefully: *"I maintain relationships with champions' managers and keep them informed about their employees' contributions. When a champion does something particularly valuable, I send their manager a brief note explaining the impact. At our annual engineering leadership meeting, we have champions present on programme outcomes and lessons learned. This visibility means leadership understands programme value whilst champions gain recognition beyond just the security team."*

The Invisible Champion Problem

Champions can be highly effective within their teams whilst remaining invisible to broader leadership. This invisibility limits their career progression and makes the programme vulnerable during budget discussions, as leadership doesn't see the champions' contributions directly. Deliberately create visibility through presentations, case studies, and leadership engagement. Champions should be known for their contributions to security beyond their immediate teams.

Navigating Common Challenges

Every programme encounters predictable challenges. Knowing they're coming helps you handle them effectively rather than being blindsided.

The Enthusiasm Drop

Most champions start with high enthusiasm. After two to three months, that enthusiasm naturally moderates as the novelty fades and the work becomes routine. Some programme leaders panic when this happens, assuming it signals programme failure.

It doesn't. It signals normalisation. The key is ensuring that enthusiasm moderates into sustainable engagement rather than dropping into disengagement.

Acknowledge this transition explicitly. Tell champions during onboarding that initial enthusiasm will moderate, and that this is normal and healthy. Frame sustained engagement as the goal rather than maintained excitement.

Ensure the transition from excitement to routine includes sufficient value and recognition to maintain motivation. Champions should be developing visible capability, achieving meaningful impact, and receiving appropriate recognition as enthusiasm normalises.

Watch for enthusiasm dropping below sustainable engagement into actual disengagement. That requires intervention. But moderate enthusiasm, accompanied by consistent participation, is exactly

The Three-Month Check-In

Schedule mandatory check-ins with all champions around their third month. Ask how they're finding the experience, what value they're getting, what challenges they're facing, what support they need. This timing catches the enthusiasm transition and lets you address concerns before they become disengagement. It also signals that you care about champions' experience throughout their journey, not just at the beginning.

what you want in the long term.

Scope Creep and Boundary Violations

As champions become more capable, demands on them tend to increase. The security team wants them to do more. Their teams expect faster responses. Programme leadership envisions broader responsibilities. Collectively, these expectations can overwhelm champions.

Protect champions from excessive scope creep. Monitor whether actual time commitments exceed stated expectations. Push back on stakeholders who try to expand champion responsibilities without acknowledging the increased burden.

Watch for boundary violations where champions are asked to do work that should remain with the security team. Champions are conducting penetration testing. Champions making high-stakes security decisions. Champions handling incident response coordination. These typically exceed the champion's appropriate scope.

Clear role boundaries help, but you also need to actively defend those boundaries when they're challenged. This requires programme leadership that advocates for champions rather than automatically agreeing to stakeholder requests.

David learned this through experience: *"After about a year, our champions were being pulled in multiple directions. The security team wanted them in every security review. Product managers wanted instant security guidance. Engineering leadership wanted them to lead major security initiatives. All reasonable desires are collectively unsustainable. I had to explicitly push back and remind everyone that champions have primary roles beyond championing. We clarified boundaries, and I started saying no to requests that would overburden champions."*

The Knowledge Hoarding Trap

Some programme leaders, especially those who built programmes from scratch, unconsciously hoard programme knowledge. They're the only ones who fully understand how things work, know the history of decisions, or possess critical relationships.

This creates single points of failure. If the programme leader leaves or becomes unavailable, the programme struggles because nobody else has sufficient knowledge to sustain it.

Deliberately distribute programme knowledge. Document key processes, decisions, and contacts. Train backup programme leadership who can sustain operations if you're unavailable. Share

programme history and context with security team members and experienced champions.

This distribution protects the programme whilst also developing others' leadership capability. Some of your champions may become future programme leaders if they've been exposed to how the programme operates.

The Bus Factor

The "bus factor" describes how many team members must be hit by a bus before a project becomes unsustainable. Many Security Champions programmes have a bus factor of one: if the programme leader disappears, the programme collapses. Deliberately increase your programme's bus factor. Could the programme continue if you were unavailable for three months? If not, identify what knowledge and capabilities need to be distributed, then systematically distribute them.

Dealing with Champion Underperformance

Not every champion thrives. Some struggle to develop capability despite support. Others don't invest sufficient time. Some give incorrect security guidance or create friction in their teams.

Address underperformance directly but supportively. Start with understanding whether there are addressable causes. Is the

champion overwhelmed with other work? Do they need different training approaches? Are they unclear about expectations?

If causes are addressable, provide targeted support. Additional mentoring, revised expectations, adjusted responsibilities. Give champions opportunities to improve by providing clear feedback on what needs to change.

If underperformance persists despite support, help the champion transition out gracefully. Make it clear that their departure isn't a failure, but a recognition that this role doesn't fit their current situation. Some champions who struggle now might be excellent champions later when their circumstances change.

Sarah manages this carefully: *"When champions aren't performing well, I have direct conversations about what I'm observing and what needs to change. Usually, these conversations lead to improvement or voluntary transition. Occasionally, I need to ask someone to step down, which is difficult but necessary. One underperforming champion who provides incorrect guidance undermines the programme's credibility more than ten excellent champions build it up."*

The Performance Conversation Framework

When addressing underperformance, use a clear framework: describe specific observations *("I've noticed you haven't participated in community discussions in three months"),* explain why it matters ("*Champion community is where most learning happens*"), and ask for their perspective ("*What's making participation difficult?"*). identify needed changes *("I need to see you actively participating at least twice monthly"*) and offer support *("How can I help make that possible?"*). This approach is direct whilst remaining supportive.

Sustaining Momentum

Initial momentum is exciting but exhausting. Long-term success requires finding a sustainable pace that maintains progress without burning out.

The Marathon Mindset

Building an effective Security Champions programme takes years, not months. This can be discouraging when you want fast results. It can also be liberating because it reduces pressure to accomplish everything immediately.

Adopt a marathon mindset. You're not sprinting toward a finish line but running a race with no defined end. Pace yourself. Celebrate incremental progress. Accept that some things will take longer than you'd like.

This mindset also helps champions. If they view championing as a sprint, they'll burn out quickly. If they view it as a marathon where consistency matters more than intensity, they'll sustain engagement.

Michael reflects on his three-year journey: "*The first year, I was frantic, trying to accomplish everything immediately. It was exhausting and probably less effective than it could have been. In year two, I settled into a steadier rhythm. Year three, I can see the compounding benefits of sustained effort. The programme doesn't require the same level of intensity as it did initially, but it does require consistent attention. That's much more sustainable.*"

Knowing When to Say No

Programme leaders face constant requests. Expand to more teams. Add new training modules. Take on additional responsibilities. Produce more reporting. Each request seems reasonable individually, but collectively they overwhelm.

Develop the capacity to say no or not yet. Every yes to something new is a no to something else, often to things you're already doing that are working well.

Evaluate requests against programme priorities. Does this request advance core programme goals? Does it create value proportional to the effort required? Do you have the capacity to do this well?

Learn to say *"That's interesting and potentially valuable, but not right now. Let's revisit after we've accomplished X."* This preserves relationships whilst protecting your capacity.

Building Programme Resilience

Resilient programmes withstand challenges that would cripple less robust ones. Leadership changes, budget pressures, organisational restructures. You can't prevent these challenges, but you can build resilience that lets you weather them.

Resilience comes from:

Distributed leadership. Multiple people who understand the programme and can sustain it if primary leadership changes.

Demonstrated value. Clear evidence of programme contribution that makes it hard to cut even when budgets tighten.

Strong relationships. Connections to stakeholders across the organisation who will advocate for the programme when it's threatened.

Flexible design. Ability to scale up or down based on resources whilst maintaining core values.

Community strength. Champions who are invested in the programme's success and will help sustain it through challenges.

Build these elements deliberately over time. The resilience you create in good times protects the programme when bad times inevitably arrive.

Rachel's programme survived a major restructure: *"When our organisation went through a restructure that eliminated several departments, our programme survived despite budget cuts elsewhere. We survived because we had strong relationships across multiple departments, clear evidence of value, and distributed leadership. Champions advocated for the programme to their new managers. Security leadership defended it to executives. We scaled down but didn't disappear. That resilience came from deliberate investment in relationships and value demonstration over the previous two years."*

Avoiding Common Mistakes

Some mistakes appear in nearly every programme. Learning from others' experiences helps you avoid repeating them.

Over-Engineering the Programme

The temptation is to create elaborate programme structures with multiple champion tiers, complex governance, detailed processes for every situation, and comprehensive documentation for all activities.

This over-engineering creates several problems. It requires significant ongoing maintenance effort. It makes the programme feel bureaucratic rather than enabling. It creates rigidity that prevents adaptation. It overwhelms champions with process rather than empowering them with capability.

Start simple. Create the minimum viable programme structure that enables champions to be effective. Add complexity only when its absence creates clear problems. Many programmes that look simple are more effective than elaborate ones because they're easier to operate and more adaptable.

James initially built complex programme structures: *"We had champion levels, progression criteria, formal governance boards,*

elaborate processes. It felt professional but required a great deal of effort to maintain. When I simplified the programme to 'champions' with clear core responsibilities and flexible optional activities, it became easier to run, and champions found it easier to engage. Sometimes less really is more."

Neglecting the Cultural Element

Some programme leaders focus entirely on technical security training whilst neglecting the cultural and interpersonal aspects that determine whether champions can influence their teams effectively.

A champion who understands security technically but can't persuade teammates to adopt secure practices delivers limited value. A champion who can have productive conversations about security concerns is valuable even if their technical expertise is still developing.

Invest in developing champions' communication, influence, and collaboration capabilities alongside their technical security knowledge. Teach them how to have difficult conversations about security trade-offs. Help them learn how to build support for security improvements. Support their development of political awareness that helps them navigate organisational dynamics.

The most effective champions are often those who combine reasonable security knowledge with excellent people skills, not those with deep security expertise but poor communication.

The Technical Expert Trap

Several programmes recruited only their most technically sophisticated engineers as champions, assuming that technical expertise would translate into effective championing. Many of these technical experts struggled because they couldn't translate their knowledge into influence within the team. They became frustrated when teammates didn't immediately adopt their security guidance. Meanwhile, champions with moderate technical skills but strong communication abilities were more effective because they could meet teams where they were and build genuine support for security improvements.

Treating All Champions Identically

Champions have different motivations, capabilities, contexts, and constraints. Treating them all identically ignores this diversity and reduces programme effectiveness.

Some champions want deep security specialisation. Others want broad general knowledge. Some have time to invest heavily. Others

can only maintain baseline participation. Some work in mature teams that can absorb sophisticated security practices. Others work in less mature contexts requiring more fundamental improvements.

Design flexibility into your programme. Core expectations everyone meets, with multiple pathways for additional contributions. Recognition that varies across different champion contexts. Development opportunities that address varied interests and needs.

This flexibility doesn't mean lowering standards. It means acknowledging that excellent championing looks different in different contexts and that one-size-fits-all approaches often fit nobody well.

Measuring Only Security Outcomes

Some programmes measure only security outcomes (e.g., incidents prevented, vulnerabilities found), whilst ignoring champion experience and programme health.

This creates blind spots. You might achieve good security outcomes whilst champions are burning out, which isn't sustainable. You might maintain high champion satisfaction whilst delivering insufficient security value, which won't maintain executive support.

Measure security outcomes and champion experience and programme sustainability. All three matter. Optimising only one dimension often degrades others.

Knowing Your Context

Generic best practices help, but every organisation is unique. The most successful programme leaders develop a deep understanding of their specific context and adapt approaches accordingly.

Reading Your Organisation

Understanding your organisation's actual culture, not its aspirational culture, determines what approaches will work.

Pay attention to how other initiatives succeed or fail in your organisation. If grassroots efforts typically struggle without executive

The Balanced Scorecard

Maintain a simple balanced scorecard with metrics across three dimensions: security impact (incidents, vulnerabilities, process improvements), champion health (engagement, retention, satisfaction), and programme sustainability (stakeholder satisfaction, resource adequacy, leadership support). Review all three dimensions quarterly. If any dimension is declining, investigate and address before it becomes a crisis.

mandate, your champions programme probably needs stronger top-down support. If employees resist anything that feels bureaucratic, keep your programme lightweight and flexible. If people value formal recognition, invest in that. If informal peer recognition matters more, focus there.

Watch what gets rewarded. If people who volunteer for additional responsibilities get praised and promoted, champions will view their role as a valuable professional contribution. If people who focus narrowly on their defined roles get ahead whilst those who spread themselves thin struggle, champions will feel penalised for their security work.

Listen to what concerns people raise. If workload concerns dominate conversations, be especially careful about time expectations. If career development anxiety is high, emphasise how championing builds valuable capabilities. If political navigation is challenging, help champions develop those skills.

Your organisation's context shapes what's possible more than any framework or best practice from elsewhere.

The Culture Transplant Failure

A financial services company tried to implement a champions programme based closely on a model from a successful technology

company. The tech company's model emphasised volunteer participation, minimal process, and grassroots cultural change. This model completely failed in the financial services culture that valued formal mandates, clear processes, and top-down change. Only after abandoning the imported model and designing for their actual culture did the programme succeed. Best practices from elsewhere are reference points, not templates to copy.

Playing to Your Strengths

Every organisation has strengths you can leverage. Identify yours and build on them rather than fighting weaknesses.

If your organisation has a strong engineering culture, leverage that through technically sophisticated security training. If you have a great training infrastructure, use it rather than building separate champion training. If people love competitive challenges, gamify aspects of security learning. If your organisation values data-driven decisions, invest heavily in measurement and evidence.

Sophie's organisation had strong community-building capability but weak formal training infrastructure: *"Rather than trying to build elaborate training programmes that would struggle in our environment, I focused on community learning. Champions learned from each other through discussions, shared examples, peer review,*

and collaborative problem-solving. This played to our organisational strength in building communities rather than fighting our weakness in formal training delivery."

Understanding Your Constraints

Every organisation has constraints. Budget limitations, workload pressures, political complexities, and regulatory requirements. Effective programme leaders work within constraints rather than pretending they don't exist.

If the budget is tight, design low-cost programme elements. Community-based learning costs little. Champions teaching each other is free. Measuring what's already been collected is cheaper than collecting new data.

If people are time-pressured, minimise time requirements and maximise value from each minute invested. If politics are complex, invest time in understanding stakeholder dynamics and navigating them carefully. If regulations constrain flexibility, work within regulatory boundaries rather than fighting them.

Constraints aren't excuses for inaction, but they do shape what approaches are viable. Acknowledging constraints honestly whilst designing creatively within them often produces more innovation than having unlimited resources.

The Long View

Security Champions programmes compound their value over time. The programme in year three delivers far more value than the programme in year one, not just because it's larger but because capabilities, relationships, and culture have matured.

Patience with Progress

Meaningful culture change takes years. Security thinking becoming the default behaviour rather than a deliberate effort requires sustained reinforcement. Champions who develop deep expertise require extensive experience.

Celebrate progress whilst accepting that some outcomes require extended timeframes. Teams won't transform overnight. Champions won't become security experts in a matter of months. Organisational culture won't shift fundamentally in one year.

This patience doesn't mean accepting slow progress unnecessarily. It means having realistic expectations about how long genuine, sustainable change takes, whilst maintaining consistent effort toward it.

Michael reflects after three years: "Year one felt slow. We were building foundations whilst seeing a limited visible impact. Year two

momentum built as foundations enabled acceleration. Year three, the programme largely runs itself whilst delivering significant value. Early investment in fundamentals paid off, but required patience to realise the benefits. Programmes that focus only on quick wins often struggle in years two and three when those fundamentals are missing."

Thinking in Generations

Your programme will likely outlast your involvement. Think about what comes after you.

Document not just what you do but why you made key decisions. Future programme leaders will benefit from understanding the reasoning behind programme design choices.

Develop potential successors so the programme doesn't depend entirely on you. Share programme knowledge, involve others in decisions, and create opportunities for others to lead aspects of the programme.

Build programme resilience that survives leadership transition. Strong documentation, distributed knowledge, clear processes, robust community. These elements ensure the programme can continue if you move to other roles.

This long view changes how you build programmes. You're not just creating something that works now, but something that can evolve and improve long after you're no longer leading it.

The Legacy Question

Ask yourself: "If I left this role in six months, would the programme continue effectively?" If not, what needs to change to make that possible? This question surfaces dependencies on you personally and helps you address them. The most successful programme leaders make themselves progressively less essential whilst making their programmes progressively more valuable.

Celebrating the Journey

Building a Security Champions programme is hard work with frequent challenges and occasional setbacks. It's also rewarding work that materially improves your organisation's security whilst developing people's capabilities and influencing organisational culture.

Acknowledge progress regularly. When champions develop new capabilities, recognise it. When security posture improves, celebrate it. When challenges are overcome, appreciate the effort that went into overcoming them. When mistakes provide learning, value the lessons gained.

This celebration isn't naive positivity that ignores problems. It's recognition that sustained effort toward meaningful goals deserves acknowledgement even when perfection remains distant.

Programme leaders who maintain this perspective tend to sustain their own engagement whilst helping champions and stakeholders stay motivated through inevitable difficult periods.

Rachel's reflection: "*Three years in, I'm proud of what we've built. Not because it's perfect, but because it's making a real difference. Champions who joined with minimal security knowledge are now security leaders in their teams. Incidents are declining. Security is part of how we think about technology, not an afterthought. It took longer than I expected and required more learning than I anticipated. But seeing the impact makes all the effort worthwhile.*"

Final Wisdom

If there's one overarching lesson from programme leaders who've built successful Security Champions programmes, it's this: stay focused on what really matters.

Elaborate frameworks, sophisticated metrics, impressive documentation, and perfect processes are less important than engaged champions who develop capability and improve security

within their teams. Everything else serves that core purpose, or it's a distraction.

When decisions are complex, ask: *"Does this help champions be more effective?"* If yes, prioritise it. If no, question whether it's worth doing.

When challenges arise, ask: *"Does this undermine champions' effectiveness or just create inconvenience?"* If the former, address urgently. If the latter, it may not need immediate attention.

When opportunities emerge, ask: *"Will this enhance champion impact or just expand programme size?"* Growth without impact is empty activity.

The programmes that succeed long-term are those that maintain relentless focus on champion effectiveness whilst adapting everything else as needed. Structures, processes, measurements, and strategies all serve the fundamental goal of enabling champions to improve security in their contexts.

Stay grounded in that purpose, and you'll navigate challenges, avoid common pitfalls, and build something genuinely valuable.

The next chapter brings these principles to life through case studies from organisations that built successful Security Champions programmes. You'll see how different contexts shaped different

approaches, what worked in practice, what didn't, and what lessons emerged that might inform your own programme design.

PART IV: LEARNING FROM EXPERIENCE

Chapter 8: Case Studies from the Field

Theory provides direction. Practice reveals reality. This chapter presents case studies from organisations that built Security Champions programmes in diverse contexts, each with different challenges, constraints, and outcomes.

These aren't sanitised success stories. They include mistakes, setbacks, and lessons learned through experience. Some programmes achieved impressive results quickly. Others struggled initially before finding approaches that worked. One collapsed entirely before being rebuilt more successfully.

Each case study explores what the organisation tried, why they made those choices, what worked, what didn't, and what lessons emerged that might inform your own programme design. While your context will differ from these examples, the patterns and principles often transfer across situations.

Case Study 1: TechForward (Mid-Sized Tech Company)

Context

TechForward is a 450-person software company providing business analytics tools to enterprise customers. They operate in a competitive market where product velocity matters, but a security breach could destroy customer trust and the business.

When Rebecca joined as Head of Security in 2022, she found capable engineers who viewed security primarily as the security team's responsibility. Security reviews were conducted late in development, often uncovering issues that required significant rework. The three-person security team was overwhelmed by review requests and couldn't provide timely guidance.

Rebecca needed to distribute security capability across engineering teams whilst maintaining the security team's sanity. She had executive support in principle, but a limited budget for new headcount. Champions seemed like the right approach, but she'd never run such a programme before.

What They Did

Rebecca started by recruiting eight champions from engineering teams that were either the most security-critical or the most open to

change. She deliberately avoided aiming for complete coverage immediately, instead focusing on building something that worked before expanding.

She invested heavily in these initial champions. Weekly office hours where she was available to answer any questions. A dedicated Slack channel where champions got priority responses. Monthly workshops covering practical security topics specific to TechForward's technology stack.

Rather than creating elaborate training materials, Rebecca taught through real examples. Recent security issues found in code reviews. Vulnerabilities discovered in dependencies. Design decisions that introduced risk. Champions learned security concepts through analysing actual situations they'd encounter in their work.

She also gave champions a clear, limited scope. They weren't expected to become security experts. They were expected to spot common security issues in their teams, ask good security questions in design discussions, and know when to escalate concerns to the security team.

After six months with the initial eight champions, Rebecca expanded to fifteen, then to twenty-five over the following year. Early champions helped recruit and train later cohorts, distributing leadership whilst reinforcing their own expertise through teaching.

What Worked

The limited initial scope. By starting with eight committed champions rather than trying to recruit thirty immediately, Rebecca could provide intensive support that quickly built confidence and capability. These champions became visible examples of the programme's value, making subsequent recruitment easier.

Learning through real examples. Champions found it easier to learn from actual TechForward code and design decisions than from generic training materials. They could immediately apply what they learned because they recognised the patterns in their daily work.

Clear boundaries. Champions knew they weren't expected to become security experts or handle complex security decisions. This realistic scope prevented overwhelm whilst creating clear expectations about when to engage the security team.

Organic expansion. Growing the programme gradually, based on demonstrated value, prevented the chaos that can come from rapid scaling. Each expansion cohort joined a programme with proven approaches rather than joining an experiment.

The Initial Investment Payoff

Rebecca's intensive support for the first eight champions required a significant time investment, approximately 8-10 hours per week in the first three months. Many programme leaders would view this as unsustainable. But the investment paid off rapidly. By month four, champions were handling security questions that would have gone to the security team, saving more time than Rebecca was investing. By month six, those eight champions had reduced the security team's review burden by approximately 30% whilst catching issues earlier when they were cheaper to fix.

What Didn't Work

The monthly champion meetings. Rebecca initially scheduled mandatory monthly meetings where all champions gathered for updates and training. Attendance was mediocre, and champions reported that the meetings felt like obligations rather than sources of value.

She experimented with different formats before eventually cancelling regular meetings entirely. Instead, she ran quarterly hands-on workshops that champions actually wanted to attend and relied on office hours and Slack for ongoing support. Engagement improved significantly.

The champion tier system. Rebecca initially created three champion levels (Associate, Champion, Senior Champion) with progression criteria. This created bureaucracy without adding value. Champions cared more about developing actual capability than advancing through formal tiers.

She simplified to just "champions" with no formal levels. Champions naturally developed varying levels of expertise, but the formal tier system added complexity without benefit.

Over-emphasising metrics. Rebecca spent significant effort in the first year building elaborate measurement systems. She tracked fifteen different metrics and produced detailed monthly reports. Most of this data wasn't useful for decisions, and the collection effort was burdensome.

She simplified to five core metrics, tracking them quarterly rather than monthly. Measurement became sustainable whilst still providing sufficient insight into programme health.

Key Outcomes After Two Years

Twenty-five active champions covering all major engineering teams. Security issues in production decreased by 62% in champion teams compared to pre-programme baselines. Issues found during design

or development increased from 28% to 71%, indicating earlier detection. Champion retention after twelve months was 84%.

More importantly, the culture shifted. Design discussions routinely included security considerations. Engineers asked security questions proactively rather than avoiding security until reviews. Security became integrated into how teams worked, rather than being a separate process imposed on them.

The security team's workload became more strategic. Less time on basic security reviews, more time on complex security architecture and emerging threats. The security team viewed champions as force multipliers rather than additional burdens.

Lessons Learned

"Start smaller than you think you should," Rebecca reflected. *"I*

The "Good Enough" Principle in Action

TechForward's programme succeeded partly because Rebecca focused on "good enough" rather than perfect. Her training was sufficient to develop practical skills, even if it wasn't comprehensive. Her measurement was sufficient to demonstrate value, even if it wasn't rigorous. Her processes were good enough to function even if they weren't polished. This pragmatism let her launch quickly, learn from experience, and iterate based on reality rather than spending months perfecting something that would need revision anyway.

wanted to launch with twenty champions immediately. Starting with eight felt underwhelming. But it was exactly right. I could support them well, they became effective quickly, and they demonstrated value that made expansion straightforward."

"Also, don't let perfect be the enemy of good. I wasted time on elaborate programme elements that didn't matter. Simple things done well beat sophisticated things done poorly. Focus on champion effectiveness, not programme impressiveness."

"Finally, listen to champions about what they need. I designed the training I thought they needed. They told me what they actually needed, which was different. When I started listening and adapting, the programme became much more effective."

Case Study 2: GlobalBank (Large Financial Services)

Context

GlobalBank is a multinational financial institution with approximately 8,000 technology staff across fifteen countries. They operate in a heavily regulated environment where security and compliance failures can result in massive fines and reputational damage.

When Marcus joined as CISO in 2021, security capability was concentrated in a 45-person central security team. Business units

had minimal security expertise, which created bottlenecks when the security team had to review everything, whilst business units lacked understanding of why security requirements existed.

Marcus had strong executive support and a reasonable budget, but faced a complex challenge: how to distribute security capability across a massive, geographically distributed, culturally diverse organisation with strong audit and compliance requirements.

What They Did

Marcus recognised that GlobalBank's hierarchical culture and compliance focus required a different approach than typical technology company champions programmes. Rather than emphasising volunteer participation and grassroots cultural change, he built a more formal structure with a clear executive mandate.

He created clearly defined champion roles with formal position descriptions, explicit time allocations (5-7% of work time), and manager approval requirements. Champions weren't volunteers who squeezed security into their existing workload; they were employees with formal security responsibilities acknowledged in their role expectations.

The programme launched regionally. Ten champions in the UK, ten in the US, and eight in Singapore initially. Each region had a programme

coordinator who adapted the core programme to the local context whilst maintaining consistency with global standards.

Training was comprehensive and certification-based. Champions completed a formal six-week training programme covering regulatory requirements, security fundamentals, risk assessment, and escalation procedures. They received certification upon completion, which carried weight in GlobalBank's credential-focused culture.

Marcus also established clear governance. A steering committee with representatives from security, compliance, audit, technology leadership, and business units. Monthly regional coordination meetings. Quarterly global champion sessions. This structure felt bureaucratic to outsiders but provided the clarity and legitimacy that GlobalBank's culture valued.

What Worked

The formal mandate. Making champions' responsibilities explicit and getting manager approval gave champions legitimacy and time allocation, rather than requiring them to volunteer additional effort. Champions could engage meaningfully because their managers expected it.

The regional structure. Rather than trying to run one global programme, the regional approach allowed adaptation to local contexts whilst maintaining core consistency. Regional coordinators understood local cultures, languages, and business practices in ways central programme leadership couldn't.

The certification approach. In GlobalBank's culture, formal certification signalled credibility and capability. Champions took the training seriously because it resulted in a recognised credential. Other employees respected certified champions more than they would have respected volunteers with informal training.

The governance structure. While outsiders viewed GlobalBank's governance as heavy, it provided the oversight and coordination that their regulated environment required. It also gave champions clear escalation paths and ensured senior leadership visibility into programme activities.

Cultural Adaptation

The lesson isn't that one approach is superior but that effective programmes adapt to organisational culture rather than importing generic best practices. GlobalBank's formal structure matched their hierarchical, compliance-focused culture. TechForward's informal approach matched their agile, engineering-led culture. Both programmes succeeded because they worked with their cultures rather than against them.

What Didn't Work

The initial global coordination overhead. Marcus's first attempt at global coordination involved monthly calls with all champions globally. With 28 champions across three continents and seven time zones, finding meeting times was impossible. Attendance was poor, and the calls felt like an obligation rather than a value.

He shifted to regional monthly calls with quarterly global asynchronous updates. This worked much better for a distributed organisation.

The comprehensive wiki. The security team built an extensive wiki with security guidance, policies, standards, and procedures. Champions rarely used it because finding relevant information in hundreds of pages was difficult.

They replaced the comprehensive wiki with focused, role-specific quick reference guides. A two-page guide for champions reviewing API designs. A three-page guide for cloud security considerations. A one-page escalation flowchart. These targeted resources got used because they were accessible and actionable.

The uniform capability expectations. Initially, all champions were expected to develop the same capabilities regardless of their roles or contexts. A champion in infrastructure faced very different

security challenges than one in application development, but both received identical training.

They segmented training and expectations by domain. Common foundational training for all champions, then domain-specific development for infrastructure champions, application security champions, data protection champions, and identity management champions. This specialisation increased the effectiveness of champions in their specific contexts.

Key Outcomes After Two Years

Fifty-eight active champions across twelve countries. Security reviews that previously took three weeks now average eight days because champions prepared their teams better and handled preliminary reviews. Compliance violations decreased by 47% in areas covered by champions. Security training completion across all technical staff increased from 63% to 89% because champions reinforced training in their teams.

More significantly, the dialogue between business units and security improved. Champions translated security requirements into a business context and explained business constraints to the security team. This bidirectional translation reduced conflict whilst improving outcomes.

The audit team noted measurable improvement in security controls, particularly in preventative controls that reduced issues before they required detective or corrective controls. This shift indicated security was becoming built-in rather than bolted-on.

Lessons Learned

"Our biggest learning was embracing our culture rather than fighting it," Marcus reflected. *"I initially wanted a lightweight, volunteer-driven programme as I'd seen in tech companies. That wasn't going to work here. Once I accepted we needed more structure and formal processes, the programme gained traction."*

"Also, regional adaptation mattered more than I expected. Our Singapore champions needed different support than our UK champions, who needed different approaches than our US champions. Trying to run everything identically globally would have

Navigating Compliance-Heavy Environments

In heavily regulated industries, champions need clear guidance on which decisions they can make and which require a formal security team review. GlobalBank created a simple decision matrix: Green (champions can decide), Amber (champions consult the security team but can proceed with guidance), Red (the security team must formally approve). This clarity prevented compliance issues whilst empowering champions to operate within appropriate boundaries.

failed. The regional coordinators who understood local contexts made the programme work."

"Finally, in compliance-heavy environments, champions need extremely clear boundaries and escalation paths. Ambiguity creates risk. Champions need to know exactly when they can decide versus when they must escalate. That clarity protects both champions and the organisation whilst enabling champions to add value within an appropriate scope."

Case Study 3: CareConnect (Healthcare Tech Startup)

Context

CareConnect is a 120-person startup building patient engagement software for healthcare providers. They're growing rapidly, securing £15 million in Series B funding in 2023, and facing increasing pressure to demonstrate robust security to enterprise healthcare customers.

Lisa, the VP of Engineering, recognised they needed better security practices but lacked resources for a dedicated security team. With regulatory requirements from HIPAA (operating in the US market) and tight budgets, she needed a cost-effective way to build security capability.

What They Did

Lisa couldn't afford to hire a CISO or build a security team. Instead, she recruited an external security consultant to work 10 hours weekly whilst building an internal champions programme to distribute security capability.

She recruited five champions from her engineering team: one from infrastructure, two from application development, one from DevOps, and one from the platform team. These weren't volunteers. She explicitly adjusted their role expectations to include security responsibilities and compensated them accordingly.

The external consultant spent half their time training and supporting champions and the other half handling complex security issues that exceeded champions' capabilities. This model provided professional security expertise whilst sustainably developing internal capability.

Training was highly practical and just-in-time. Rather than comprehensive upfront training, the consultant taught champions as they encountered actual security challenges. Real threat models for the features they were building. Actual secure coding patterns for their technology stack. Specific compliance requirements they needed to meet.

Lisa also invested in automation and tooling to make secure practices easier. Automated security scanning in CI/CD pipelines. Pre-configured secure templates for common patterns. Policy-as-code that enforced security requirements automatically. Champions focused on security decisions and guidance, whilst tools handled enforcement.

What Worked

The hybrid model. Combining external expertise with internal champions gave CareConnect the security capability they couldn't afford to hire fully, whilst building internal expertise that would become sustainable as they grew.

The compensation approach. Rather than asking engineers to volunteer additional effort, Lisa formally recognised security responsibilities through adjusted expectations and compensation. Champions viewed security work as a valued professional responsibility rather than an optional volunteer activity.

The just-in-time training. Teaching security concepts when champions immediately needed them proved more effective than upfront, comprehensive training. Champions learned in context and could apply knowledge immediately, whilst the external consultant was available for questions.

The automation emphasis. By automating routine security enforcement, champions could focus on judgment and decisions rather than manual checking. This maximised the value of limited champion time whilst ensuring consistent baseline security.

The Resource-Constrained Reality

Many organisations face CareConnect's resource constraints. They need security capability but can't afford dedicated security teams. The champions programme becomes not just a way to distribute capability but the primary security capability. This works if you're realistic about scope. Champions with external support can handle most security needs for organisations of CareConnect's size. But acknowledge limitations. Champions aren't penetration testers, incident response coordinators, or security strategists. Know when you need to bring in additional external expertise for capabilities that champions can't reasonably develop.

What Didn't Work

The community focus. Lisa tried to build a community of champions through regular meetings and active discussion channels. With only five champions, this felt forced. They interacted naturally through their daily work without needing structured community activities.

She abandoned the community-building efforts and focused on ensuring champions had access to the external consultant when

they needed help. At CareConnect's scale, the consultant relationship mattered more than a champion-to-champion community.

The comprehensive security standards. The external consultant developed detailed security standards covering all aspects of secure development. Engineers found them overwhelming and didn't use them.

They replaced comprehensive standards with minimal, actionable standards focused on the most critical requirements. A one-page secure coding checklist. A two-page cloud security guide. A three-page threat modelling template. These practical resources were used because they were accessible and sufficient.

The weekly champion sync. Lisa scheduled weekly meetings where all champions synced on security activities. These meetings often lacked substance because there wasn't always news to share.

She switched to ad hoc meetings when there was something to discuss, with a monthly optional coffee chat for informal connection. This reduced meeting burden whilst maintaining necessary coordination.

Key Outcomes After Eighteen Months

CareConnect passed healthcare customer security audits that had previously been obstacles to enterprise sales. They achieved SOC 2 Type II certification ahead of schedule. Security incidents were minimal, with only two moderate-severity issues in eighteen months (both caught before production).

More importantly, security became integrated into their development practices from the start. Threat modelling happened during design. Security testing was automated and routine. Engineers asked security questions naturally rather than viewing security as an afterthought.

The external consultant's role gradually shifted from training and support to more strategic security work as champions developed their capabilities. By month eighteen, the consultant spent about 60%

External Expertise as Accelerant

Many smaller organisations lack a budget for full-time security staff but can afford part-time external expertise. Use that external expertise to build internal capability through champions rather than handling all security work directly. The external expert's most valuable role is to develop champions who can eventually handle most security needs, with occasional external support for complex issues. This model creates sustainable security capability whilst remaining cost-effective.

of their time on strategic security work and 40% on champion support, rather than the initial 50/50 split. This evolution validated that the programme was successfully building internal capability.

CareConnect's investors viewed the security programme as a strength that positioned them well for enterprise market penetration. Security became a competitive advantage rather than a compliance obligation.

Lessons Learned

"We couldn't afford a security team, but we couldn't afford to not have security capability," Lisa reflected. *"Champions let us build what we needed within our budget constraints. The key was being realistic about scope and providing adequate support."*

"Also, at a small scale, you don't need elaborate programme infrastructure. We tried to implement practices from large organisations, and they felt ridiculous with five people. Keep it simple. Focus on effectiveness, not structure."

"Finally, automation multiplies champion impact. Every security concern we automated meant champions could focus on things requiring human judgment. In resource-constrained environments, automating what's automatable is essential to making limited champion time effective."

Case Study 4: RetailCorp (Legacy Retail Organisation)

Context

RetailCorp is a 90-year-old retail chain with approximately 2,000 technology staff supporting physical stores, e-commerce, supply chain, and corporate systems. They operate on a mix of modern cloud-based systems and decades-old legacy mainframe applications.

When David joined as Chief Information Security Officer in 2020, he found a deeply siloed organisation with limited communication between teams, resistance to change, and security viewed primarily as a compliance checkbox rather than genuine risk management.

The security team had reasonable resources but struggled to engage with business units. Security reviews were adversarial. Security requirements were seen as obstacles rather than enablers. David needed to change the relationship between security and the rest of technology.

What They Did

David recognised that RetailCorp's culture wouldn't embrace grassroots volunteer programmes. Change happened through formal channels with senior leadership support. He secured

executive sponsorship from the CTO, who mandated that each major technology department designate security champions.

Rather than recruiting volunteers, managers nominated champions from their teams. David then met with each nominated champion to explain the role, set expectations, and confirm their willingness to participate. This approach generated the top-down mandate that RetailCorp's culture required, whilst ensuring champions had a genuine interest rather than just manager pressure.

He structured the programme around departments rather than trying to create one unified champion network. Mainframe champions formed one community. Cloud applications champions formed another. Retail systems champions formed a third. E-commerce champions formed a fourth. Each community had distinct security challenges and needed different support.

David invested heavily in building relationships between champions and the security team. Monthly office hours where champions could bring questions. Paired reviews where champions and security team members reviewed designs together. Regular lunch sessions where champions and security staff connected informally. This relationship-building transformed the adversarial dynamic into collaboration.

He also created "champion champions" among senior engineers who became advocates within their departments. These informal leaders helped establish the champions' credibility whilst modelling effective security collaboration for their peers.

What Worked

The mandated nomination process. In RetailCorp's culture, volunteer programmes struggled. Getting executive mandate and manager nominations provided legitimacy that volunteer recruitment wouldn't have achieved. Champions could tell colleagues "This is part of my role" rather than "I'm volunteering for this."

The segmented communities. Rather than forcing champions working on mainframe systems to connect with champions working on cloud applications, letting them form separate communities with shared contexts meant more relevant learning and stronger relationships.

The relationship investment. Transforming the adversarial security-business relationship required sustained effort, building personal connections. The time David invested in lunches, coffee chats, and informal interactions paid off, as champions viewed the security team as partners rather than obstacles.

The champion advocates. Identifying and supporting informal leaders among champions created internal programme momentum. These advocates recruited subsequent champions, defended the programme when questioned, and modelled effective championing for others.

Changing Established Cultures

RetailCorp demonstrates that champion programmes can work in traditional, change-resistant organisations, but require different approaches than in agile, innovative cultures. Success factors included strong executive sponsorship, working through established management structures, acknowledging rather than fighting cultural norms, and patient relationship-building over time. Culture change in established organisations takes years, not months. Champions plant seeds that gradually shift how people think about security rather than forcing rapid transformation.

What Didn't Work

The comprehensive training programme. David developed a six-month training program covering all aspects of security. Champions couldn't sustain attendance alongside their regular responsibilities, and much of the training wasn't relevant to their immediate needs.

He replaced comprehensive training with targeted, on-demand learning. Short sessions on specific topics when champions needed them. Self-paced materials champions could consume when convenient. Focus on breadth (basic understanding of many topics) rather than depth (expertise in specific areas).

The unified champion community. Initial attempts to bring all champions together, regardless of their technical domains, created confusion rather than cohesion. Champions working on mainframe systems had little to discuss with champions working on mobile applications.

Segmenting into domain-specific communities whilst maintaining occasional cross-domain sessions proved more effective. Champions learned primarily within their domains whilst gaining occasional broader perspectives.

The rapid change expectations. David initially hoped to transform RetailCorp's security culture within a year. This timeline was completely unrealistic for an organisation of RetailCorp's size and cultural entrenchment.

He adjusted to a multi-year perspective. Year one: establish programme and build relationships. Year two: demonstrate value and expand. Year three: deepen impact and cultural shift. This

realistic timeline prevented discouragement whilst maintaining steady progress.

Key Outcomes After Three Years

Forty-two active champions across major technology departments. Security review cycle times decreased from an average of 19 days to 11 days because champions prepared their teams better and handled preliminary discussions. Security issues found in production declined by 38%, with most improvement coming from earlier identification in development cycles.

The relationship between security and technology departments measurably improved. Anonymous surveys showed favourability toward the security team increasing from 34% to 67%. Security requirements were increasingly viewed as helpful guardrails rather than arbitrary obstacles.

Champions became recognised technical leaders within their departments. Several champions advanced to senior or lead engineer roles, partly because of the security expertise they'd developed. This visibility motivated other engineers to become champions.

RetailCorp's audit findings decreased substantially. External audits that previously identified 40-50 issues now identify 15-20, most of

which are low severity. This improvement validated that security posture was strengthening materially.

Lessons Learned

"Working with our culture rather than against it was essential," David reflected. *"I initially wanted to create the kind of dynamic, innovative programme I'd seen in tech companies. RetailCorp wasn't that culture. Once I accepted we needed more structure, more hierarchy, more formal processes, the programme gained traction."*

"Also, relationship-building matters more than programme structure in changing adversarial dynamics. We had reasonable structures initially, but progress accelerated when I invested in personal connections between champions and security team members. Trust enables collaboration that processes alone can't create."

Patience in Large, Complex Organisations

Large organisations with established cultures, complex technical landscapes, and strong silos require a patient approach to programme building. Don't expect dramatic results quickly. Focus on steady progress: building relationships, demonstrating small wins, and gradually shifting perceptions. Three years into RetailCorp's programme, meaningful change was visible. One year in, progress seemed minimal. The lesson: maintain consistent effort without expecting rapid transformation, trust that sustained work compounds over time.

"Finally, segmentation was crucial. We have diverse technical environments, and trying to create one unified programme across all domains created confusion. Letting mainframe champions, cloud champions, and legacy application champions form separate communities whilst maintaining occasional connection worked much better."

Case Study 5: The Failed Launch (Manufacturing Company)

Context

Not every champions programme succeeds. This case study examines a programme that failed, was rebuilt, and eventually succeeded. The lessons from failure often teach more than success stories.

IndustrialTech is a 350-person manufacturing technology company providing industrial automation software. When Sarah was hired as their first Head of Security in 2021, she wanted to establish Security Champions quickly to demonstrate early impact.

What Went Wrong

Sarah made several mistakes that compounded to undermine the programme before it could establish value.

She launched too quickly. Eager to show progress, Sarah recruited 28 champions within the first month and scheduled training to begin immediately. She hadn't built relationships with engineering leadership, identified an executive sponsor, or developed a clear programme design. She just knew she wanted champions and moved fast to get them.

She underestimated the time commitment. Sarah told prospective champions the role would require "*a couple of hours monthly*." In reality, effective championing required 5-7 hours monthly. Champions felt misled and overwhelmed when they discovered the actual commitment.

She focused on compliance over enablement. Sarah's training emphasised regulatory requirements and security policies that champions must enforce. This positioned champions as security police rather than team enablers. Teams resented champion involvement rather than valuing it.

She lacked support infrastructure. Sarah was the only support for 28 champions whilst also building the security programme, conducting reviews, managing compliance, and handling incidents. She couldn't provide adequate champion support, and champions struggled without guidance.

She measured activity rather than impact. Sarah tracked champion training completion, meeting attendance, and reviews conducted. These metrics showed activity but didn't demonstrate that champions were improving security. When leadership questioned programme value, she couldn't make a compelling case.

The Rapid Launch Trap

Many new security leaders feel pressure to demonstrate quick wins. Launching a champions programme seems like an achievable early success. But programmes launched too quickly, without adequate preparation, often fail because the foundations are missing. Better to spend three months building relationships, securing sponsorship, and designing thoughtfully, then launching a sustainable programme, than to launch immediately with a programme that collapses within six months. Quick starts often lead to slow (or negative) outcomes.

The Collapse

By month four, attendance at champion meetings had dropped to about 40%. Champions stopped engaging in discussion channels. Several champions told Sarah they couldn't continue due to time pressure. Others simply disengaged without formally quitting.

The security team began complaining that champions were creating additional work rather than reducing it. Champions were

asking basic questions that showed insufficient training. They were escalating issues inappropriately. They were confusing their teams with contradictory guidance.

By month six, only eight of the original 28 champions remained nominally engaged, and most of those participated minimally. The programme had effectively collapsed.

The Rebuild

Sarah faced a choice: abandon champions entirely or learn from mistakes and rebuild. She chose to rebuild, but differently.

She started by honestly acknowledging failure to leadership and the remaining champions. *"I launched this poorly. I need to take responsibility for that and do it better."* This honesty preserved relationships and credibility.

She stepped back to do what she should have done in the first place. She secured executive sponsorship from the VP of Engineering. She built relationships with engineering managers. She designed the programme structure carefully rather than improvising. She set realistic expectations about time commitment and valued the timeline.

She recruited a fresh cohort of eight champions (including three who'd remained from the initial programme). She was transparent about the previous failure and what would be different this time.

She invested heavily in support. Weekly office hours. Active responsiveness in communication channels. Regular check-ins with individual champions. She treated champion support as her top priority rather than something she did when she found time.

She positioned champions as team enablers rather than security enforcers. Training emphasised making security easier for teammates, preventing problems that would slow delivery, and being a resource rather than an obstacle.

She measured impact rather than just activity. Security posture improvements in champion teams. Earlier issue identification. Team satisfaction with champion support. These metrics demonstrated value even when programme size remained small.

The Successful Second Attempt

The rebuilt programme started small but grew steadily based on demonstrated value. After six months with eight champions, she expanded to twelve. After a year, to eighteen. After eighteen months to twenty-four.

Retention was strong. Only two champions left the rebuilt programme in the first year, both due to role changes rather than dissatisfaction. Champions who'd been part of the initial failure and remained for the rebuild became programme advocates because they'd seen both approaches and could articulate why the second worked better.

Security posture improved measurably. Issues found during design or development increased from 23% pre-programme to 64% after eighteen months. Production security incidents in champion teams declined by 54% compared to baseline.

More importantly, champions were viewed positively. Team surveys showed that 76% of engineers with champions valued their champions' contributions. Managers appreciated champions

Learning from Failure

Programme failure isn't fatal if you learn from it and adjust. Sarah's rebuilt programme succeeded partly because she'd learned what doesn't work. She knew launching without relationships fails. She knew that underestimating time commitment undermines trust. She knew positioning champions as enforcers creates resistance. These lessons, learned through painful experience, informed better programme design the second time. If your programme struggles, an honest assessment of what's not working and a willingness to adjust substantially often lead to eventual success.

making security easier rather than harder. The security team viewed them as effective collaborators who reduced the burden.

Lessons Learned

"Failure taught me more than success would have," Sarah reflected. *"I learned that relationships and trust matter more than programme structure. I learned that setting realistic expectations prevents problems better than fixing them after they emerge. I learned that how you position champions determines whether teams embrace or resist them."*

"Also, starting small and building on success beats launching big and hoping it works. My first attempt tried to do too much too quickly. The rebuild started smaller but grew sustainably because we were building on demonstrated value rather than hoped-for value."

"Finally, admitting failure and learning from it preserves credibility. I could have hidden the initial programme's collapse or made excuses. Acknowledging it honestly, whilst demonstrating I'd learned from it, actually strengthened my relationships with engineering leadership and champions. Authenticity builds trust even when discussing failure."

Patterns Across Contexts

While these case studies represent diverse contexts, several patterns emerge across successful programmes:

Start smaller than feels comfortable. Every successful programme started with fewer champions than the leader initially wanted. This allowed intensive support, quick capability development, and demonstrated value before scaling.

Adapt to your culture. Approaches that worked in one organisational culture failed in another. TechForward's informal approach wouldn't have worked at GlobalBank. RetailCorp's mandated structure wouldn't have worked at CareConnect. Successful leaders worked with their cultures rather than importing best practices from different contexts.

Invest in relationships. Programmes that thrived built strong relationships between champions, security teams, and leadership. Programmes that struggled often had good structures but poor relationships. Relationships enable collaboration that structures alone can't create.

Measure what matters. Programmes that demonstrated value measured security outcomes and champion impact rather than just

activity. Programmes that struggled measured activity without connecting it to outcomes.

Maintain realistic timelines. Successful programmes adopted multi-year perspectives. Programmes that failed often expected dramatic results in months. Sustainable change takes time.

Learn from problems. Every programme encountered challenges. Successful programmes identified problems early, investigated causes, and adjusted approaches. Struggling programmes often recognised problems late or persisted with failing approaches.

Applying These Lessons

These case studies aren't templates to copy but examples to learn from. Your context will differ from all of these organisations. But the patterns and principles often transfer.

As you design or refine your own programme, ask yourself:

Which case study context most resembles yours? What from their approach might work in your environment? What would need adaptation?

What mistakes do you see yourself potentially making based on these examples? How can you proactively avoid them?

What success factors appear across multiple contexts? How can you incorporate those into your programme design?

What timeline seems realistic given your context? Are you expecting results faster than similar programmes achieved?

The goal isn't to replicate someone else's programme but to learn from their experiences whilst designing something tailored to your specific situation. These case studies provide reference points, not blueprints. Use them to inform your thinking whilst maintaining focus on your unique context and needs.

The final chapter looks forward to how Security Champions programmes are evolving and what the future might hold for this approach to distributed security capability.

PART V: LOOKING AHEAD

Chapter 9: The Future of Security Champions

Security Champions programmes have evolved considerably over the past decade. What began as informal arrangements where interested engineers helped with security has matured into structured programmes with defined roles, formal development paths, and demonstrated business value. But the evolution continues.

This chapter explores where Security Champions programmes are heading. The emerging trends reshaping how champions work, the new challenges they'll face, the opportunities technology creates, and the fundamental principles that will remain relevant regardless of how the landscape changes.

We're not predicting a distant future but examining forces already reshaping champions programmes today and likely to intensify over the next few years. Understanding these trends helps you build programmes that remain effective as circumstances evolve.

The Automation Paradox

Artificial intelligence and automation are transforming security practices. Some observers predict these technologies will make Security Champions obsolete. Automated tools can scan code for vulnerabilities, detect security anomalies, and even suggest fixes. Why do you need human champions when machines can do security work?

This prediction misunderstands what champions actually do.

What Automation Handles Well

Automation excels at repetitive, rule-based security tasks. Scanning code for known vulnerability patterns. Checking configurations against security standards. Monitoring for suspicious activity patterns. Enforcing security policies consistently.

These capabilities are valuable and expanding rapidly. AI-powered security tools can now identify vulnerabilities that traditional static analysis missed. They can generate secure code patterns. They can prioritise security findings based on contextual risk. They're becoming remarkably sophisticated.

This automation reduces the tactical burden on champions. They spend less time on manual security reviews and more time on activities requiring human judgment and contextual understanding.

What Requires Human Champions

Champions provide capabilities that automation can't replace, at least not in the foreseeable future.

Contextual judgement. Security isn't binary. The same architectural decision might be appropriate in one context and risky in another. Champions understand their teams' business requirements, risk tolerance, operational constraints, and strategic priorities. They make security decisions that balance competing concerns, drawing on a nuanced understanding that automation lacks.

Cultural influence. Changing how teams think about security requires trust, relationships, and communication. Automated tools can identify problems, but they can't persuade teams to care about security, build security thinking into team culture, or influence behaviours through peer relationships. This cultural work is fundamentally human.

Complex problem-solving. Novel security challenges that require creative thinking, architectural innovation, or the integration of multiple concerns won't be solved by tools that apply learned

patterns. Champions collaborate with teams to design security approaches for situations that don't fit established patterns.

Translation and communication. Security team guidance needs to be translated into the team's context. Business requirements need to be translated into security implications. Champions bridge these communication gaps in ways that maintain relationships and build understanding. Automated tools can provide information, but can't navigate the human dynamics of security communication.

The Augmentation Model

The future isn't automation replacing champions but augmenting them. Champions supported by sophisticated tools can handle more complex security challenges, support more teams, and focus on high-value activities that require human judgment. An effective champion with excellent tools can provide security guidance and support that might have required three or four champions previously. But the champion role becomes more important, not less, because humans handle aspects that automation can't address, whilst automation handles routine tasks that previously consumed the champion's time.

How Champions' Work is Changing

As automation handles more tactical security work, champions' focus is shifting toward strategic contribution.

Less time finding basic vulnerabilities. Automated scanning tools identify these effectively. Champions increasingly focus on complex security issues that tools miss or on helping teams understand and prioritise the findings tools generate.

More time on security architecture. As tactical security becomes automated, champions spend more time on architectural decisions, threat modelling, security design patterns, and strategic security improvements that require understanding business context and technical constraints.

Less time on policy enforcement. Policy-as-code and automated controls enforce many security requirements. Champions focus on helping teams understand why policies exist and how to work effectively within security constraints rather than manually checking compliance.

More time on security culture. Building teams that naturally think about security, proactively consider security implications, and collaborate effectively with security specialists requires sustained human effort. This cultural work becomes a larger part of the champion's responsibility.

Emma, who's run a champions programme for four years, sees this shift: *"Five years ago, champions spent probably 70% of their time on tactical security reviews and 30% on strategic work. Now it's inverted.*

Automated tools handle most tactical reviews. Champions spend maybe 30% of their time on tactical issues that tools flag for human judgment and 70% on architecture, culture, and strategic improvements. The role has become more sophisticated and more valuable."

The Distributed Work Reality

The shift toward remote and hybrid work, accelerated dramatically by the pandemic, fundamentally changes how champions programmes operate.

The Death of the Hallway Conversation

Many security champions' programmes historically relied on informal interactions. The champion who overhears a design

Preparing Champions for Strategic Work

If automation is shifting champions toward strategic contribution, programme development needs to emphasise strategic capabilities. Develop champions' skills in threat modelling, security architecture, risk assessment, and influence. Reduce emphasis on finding specific vulnerability types that tools now identify effectively. Train champions to interpret and contextualise tool findings rather than manually searching for issues. This development shift prepares champions for the work that automation can't handle

discussion in the office and contributes a security perspective. The team member who stops by the champion's desk with a quick security question. The impromptu whiteboard session where security architecture gets sketched out.

Remote and hybrid work eliminates these serendipitous interactions. If they're not deliberately recreated in digital forms, valuable security conversations simply don't happen.

This isn't necessarily negative. Distributed work can make programmes more inclusive and accessible. But it requires intentional design rather than assuming informal interactions will occur naturally.

New Practices for Distributed Champions

Successful programmes are adapting to distributed reality through several approaches.

Structured office hours. Instead of relying on people stopping by champions' desks, champions hold regular virtual office hours when anyone can join with questions. These scheduled sessions replace spontaneous interactions whilst being more predictable and accessible.

Async-first communication. Rather than expecting real-time discussion, programmes are designed for asynchronous collaboration. Champions document security guidance that teams can access when needed. Discussion channels where questions get answered over hours rather than minutes. Recorded training that champions can consume at convenient times.

Digital whiteboarding. Security design discussions that used to happen on physical whiteboards now occur in digital collaboration spaces. Tools like Miro, Mural, or Figma provide persistent canvases where security architectures get sketched, discussed, and refined over time rather than in single sessions.

Deliberate relationship building. Without office proximity creating natural relationship development, programmes create structured opportunities for connection. Virtual coffee pairings. Social channels for non-work discussion. Regular video calls focused on community building rather than work tasks.

Marcus runs a distributed champions programme*: "We had to completely rethink how champions connect with each other and with their teams. We schedule more deliberately. We document more thoroughly. We create more structured opportunities for interaction. The informality we lost through remote work gets replaced with intentional design. Different, but can be equally effective if you're thoughtful about it."*

The Documentation Imperative

Distributed work makes documentation far more critical. When teams are co-located, undocumented knowledge gets transferred through conversation. When distributed, what's not documented is effectively not known. Champions need to document security decisions, rationale, patterns, and guidance more thoroughly than when teams could simply ask questions face-to-face. This documentation burden is real but creates benefits: knowledge persists beyond individual champions, new team members can onboard faster, and decisions get recorded with rationale. Investment in good documentation practices pays off through better knowledge retention and transfer.

The Global Champions Network

Distributed work enables programmes to span geographies in ways that weren't previously practical. A company might have champions on five continents collaborating as one network because physical location matters less.

This creates opportunities. Broader diversity of perspectives. Access to security expertise wherever it exists in the organisation. 24-hour coverage, with someone in the Champion Network always available.

But it also creates challenges. Time zone coordination. Cultural differences in communication styles. Language barriers. Varying

regulatory contexts. Programme leaders need to navigate these complexities deliberately.

Louise manages a global champions programme: *"We operate as one programme but acknowledge our diversity. We have regional coordinators who understand local contexts. We run some sessions globally and some regionally. We create asynchronous participation options for people who can't join synchronous sessions in their time zones. We're explicit about cultural communication norms and create space for different approaches. It's more complex than managing co-located champions, but the diversity of perspectives makes us stronger."*

Integration with Other Security Practices

Security Champions programmes don't exist in isolation. They're increasingly integrating with other security practices and technologies.

DevSecOps Convergence

DevSecOps emphasises integrating security into development and operations practices. Security Champions programmes are natural enablers of DevSecOps, as champions embed security thinking into development teams.

As DevSecOps practices mature, the roles of champions often expand. They're not just providing security guidance; they're also helping implement security automation in CI/CD pipelines, configure security tools, interpret security scan results, and train teams on secure development practices.

This convergence makes champions more technical and tool-oriented than traditional security awareness roles. Champions need to understand not just security principles but also the practical implementation of security in modern development workflows.

James sees this evolution: "Our champions five years ago focused primarily on security awareness and design reviews. Our champions today are implementing security scanning tools, writing security test cases, configuring cloud security controls, and automating security checks. The role has become much more technical because security has become more integrated into technical workflows rather than being a separate review process."

Shift-Left Security

The shift-left movement pushes security earlier in development lifecycles. Rather than security reviews happening before release, security considerations are integrated into design, coding, and testing.

Champions are essential shift-left enablers. They bring security thinking to the design phases, identify security requirements during sprint planning, and incorporate security into development practices. Their embedded position allows them to shift security left in ways that centralised security teams can't.

This shift changes champion focus. Less emphasis on finding issues in completed work. More emphasis on preventing issues through secure design, secure coding practices, and security testing that happens throughout development.

Security as Code

Defining security controls, policies, and configurations as code makes security requirements explicit, version-controlled, and automatable. Champions often play central roles in implementing security-as-code practices.

They help define security policies that get codified. They implement policy enforcement in deployment pipelines. They train teams on working with security-as-code tools. They bridge between security team policy intentions and development team implementation practices.

This technical role requires champions who understand both security and infrastructure-as-code, policy frameworks, and

automated enforcement mechanisms. The bar for champion technical capability is rising.

Emerging Threat Landscapes

The threats organisations face are evolving, which shapes what champions need to focus on.

Supply Chain Security

Modern software depends on extensive supply chains of open-source packages, cloud services, and third-party components. Securing these supply chains requires vigilance about dependencies, awareness of supply chain attacks, and practices that verify component integrity.

Champions play crucial roles in supply chain security because they're positioned where dependency decisions get made. They can influence which packages teams adopt, establish practices for verifying dependencies, identify risky third-party integrations, and ensure supply chain security controls are implemented.

This wasn't a traditional focus on champions, but it is becoming increasingly important as supply chain attacks multiply.

Cloud Security Complexity

As organisations move to cloud platforms, security complexity increases. Multiple cloud providers, complex permission models, evolving services, and shared responsibility models in which security ownership is unclear.

Champions help teams navigate this complexity. They understand cloud security models, review cloud architectures for security implications, help implement cloud security controls, and translate cloud security requirements into practical team actions.

Cloud security knowledge is becoming an essential champion capability rather than specialised expertise.

AI and ML Security

As organisations deploy AI and machine learning systems, new security challenges emerge. Model poisoning, adversarial attacks, data privacy in training sets, bias amplification, and prompt injection in language models.

These risks differ from traditional security concerns and require different mitigation approaches. Champions will increasingly need AI security awareness to guide teams building AI-powered features.

Rachel is already seeing this: *"Two years ago, AI security wasn't on our champions' radar. Now, multiple teams are building features using large language models and need guidance on prompt injection risks, data privacy implications, and model deployment security. We're rapidly developing AI security capability in our champions because teams need it immediately."*

The Specialisation Question

As security domains multiply and deepen, a question emerges: should champions be security generalists with broad basic knowledge, or specialists with deep expertise in specific domains? The answer likely depends on organisation size and complexity. Smaller organisations need generalist champions who can address diverse security concerns. Larger organisations may benefit from specialist champions focused on specific domains like cloud security, application security, or AI security. Most programmes will likely develop a core of generalists supplemented by specialists for complex domains.

The Professionalisation of Champions

Security Champions programmes are maturing from informal volunteer arrangements into recognised professional roles with career paths and formal development.

Champions as a Career Path

Increasingly, organisations recognise championing as a valuable professional contribution that should connect to career advancement. Champions who develop deep security expertise can progress toward formal security roles. Others use security expertise to advance in their primary disciplines as engineers who understand security are increasingly valuable.

Some organisations are creating formal "security engineer" roles that combine development and security responsibilities. Champions are natural candidates for these hybrid roles because they've already demonstrated the ability to operate at the intersection of development and security.

This professionalisation benefits programmes by attracting ambitious engineers who view champions as a means of career development rather than as additional volunteer work. It also raises expectations. Champions who view the role as a professional responsibility bring higher commitment than volunteers who treat it as an optional side project.

Certification and Credentialing

Security certifications are proliferating. Some organisations are developing internal champion certifications. Industry bodies are

creating credentials specifically for security champions or similar roles.

This formalisation provides benefits. Clear development paths. External validation of capability. Recognition that transfers beyond individual organisations. But it also risks over-emphasising credentials at the expense of practical effectiveness.

The most successful approaches balance formal certification with demonstrated capability. Certifications provide useful frameworks for development, but don't substitute for actual security contribution and team impact.

Michael's organisation developed an internal certification: *"We created a three-level champion certification based on demonstrated capabilities and contributions. Associates who've completed foundation training and are actively championing in their teams. Champions who've demonstrated strategic security contribution over sustained periods. Senior Champions who've mentored others and driven significant security improvements. These levels provide recognition and progression whilst ensuring certification reflects actual capability rather than just training completion."*

Champions as Security Professionals

An interesting evolution is champions who transition fully into security roles whilst maintaining their embedded team positions. These hybrid roles combine membership on the security team with continued integration into development teams.

This model provides benefits. Security expertise is embedded where decisions are made. Development perspective informing the security team's thinking. Career path for champions who want to specialise in security without leaving their teams.

It also requires careful design. How do these hybrid roles balance the responsibilities of the security and development teams? Who manages them? How do their metrics and incentives align? Organisations experimenting with this model are still working through these questions.

The Relationship with Central Security

The relationship between Security Champions programmes and central security teams is evolving in interesting ways.

From Support to Partnership

Early champions programmes often positioned champions as helpers or extensions of the security team. Champions did the work the security team needed done, but lacked the capacity to do.

Increasingly, the relationship is shifting toward a genuine partnership. Champions aren't junior members of the security team; they're professional peers with different roles and perspectives. They provide insights the security team lacks about how teams work, what's practical to implement, and where security friction arises.

This partnership model changes how programmes operate. Champions have more autonomy and authority. Security teams learn from champions rather than just teaching them. Programme design becomes collaborative, rather than the security team designing everything and the champions executing.

David sees this shift: *"Initially, our security team told champions what to do and how to do it. Now it's much more collaborative. Champions bring perspectives that inform security team decisions. They identify security approaches that won't work in practice before we implement them. They help design security requirements that are both effective and practical. They're partners in security strategy, not just implementers of security team directives."*

Distributed Security Ownership

Traditional models concentrated security ownership in central security teams. Champions programmes distribute that ownership more broadly. Security becomes a shared responsibility between central security, champions, and development teams.

This distribution creates benefits. Security decisions informed by broader perspectives. Faster security responses because champions are embedded rather than external. Security thinking is integrated throughout the organisation rather than concentrated in one team.

But it also creates complexity. Who makes final security decisions when champions and security teams disagree? How do you maintain security consistency whilst enabling distributed ownership? What authority do champions have versus what remains with central security?

Successful programmes navigate these questions through clear decision frameworks, strong relationships built on trust, and processes that balance consistency with distributed authority.

The Authority Ambiguity

One ongoing challenge is ambiguity about champion authority. Are champions advisors who provide guidance but don't make decisions? Are they decision-makers within certain boundaries? Are they security team representatives with delegated authority? Different programmes answer differently, and there's no universally correct answer. But the ambiguity itself creates problems. Champions and teams need a clear understanding of what champions can decide versus what requires security team involvement. Make this explicit rather than leaving it ambiguous.

Sustainability Challenges Ahead

As programmes mature, they face sustainability challenges that weren't apparent during early enthusiasm.

Avoiding Stagnation

Mature programmes risk stagnation. What felt innovative and energising initially becomes routine and administrative. Champions who joined when the programme was new and exciting find it's now established and somewhat bureaucratic.

Preventing stagnation requires continuous evolution. Refreshing programme elements periodically. Introducing new challenges and opportunities for champions. Ensuring experienced champions find

continued development and engagement rather than repeating the same activities indefinitely.

Programmes that stay vital over the years are those that evolve whilst maintaining their core purpose.

Maintaining Executive Support

Initial executive enthusiasm often wanes as programmes become established. Early novelty and visible launches generate excitement. Mature programmes that deliver steady value are less exciting, even if they're more valuable.

Maintaining executive support requires demonstrating ongoing value, connecting programme outcomes to business priorities, and ensuring leadership is aware of champions' contributions. It also requires avoiding complacency. Don't assume executive support will persist automatically just because the programme has worked in the past.

Rachel actively maintains executive engagement: *"Every quarter, I update our executive sponsor on programme impact, but I also ask for their input and perspective. What security concerns keep them up at night? What business objectives does security need to enable? How can champions contribute to strategic priorities? This dialogue*

keeps them engaged whilst ensuring our programme stays aligned with what matters to leadership."

Resourcing Sustainably

Many programmes launch with enthusiasm that generates resources, then struggle to maintain funding as novelty fades. Programmes need sustainable resourcing models that don't depend on constant justification to sceptical stakeholders.

This requires building the programme's value case so strongly that cutting funding becomes obviously foolish. It also requires managing costs to remain within budgets that can be sustained through normal business cycles rather than requiring special funding.

Efficient programme design matters for sustainability. Programmes that deliver value without requiring extensive ongoing investment are more sustainable than those that demand constant resources to maintain.

The Core That Won't Change

Despite all these evolving trends, certain fundamental principles will remain relevant regardless of how technology, threats, or organisational practices change.

Security is Still About People

Technology changes rapidly. Security tools evolve. Threats shift. But security remains fundamentally about human decisions and behaviours. People decide whether to click suspicious links, whether to implement security requirements properly, whether to take shortcuts under pressure, whether to report concerns or stay silent.

Champions influence these human decisions and behaviours. That role will remain relevant regardless of technological evolution. Automated tools can enforce policies and detect anomalies, but influencing security culture requires human connection and communication.

Distributed Beats Centralised

Central security teams will always have important roles in strategy, specialised expertise, and organisational coordination. But they can't scale to provide security guidance at every decision point across large organisations.

Distributed security capability through champions provides reach and speed that central teams can't achieve. This fundamental advantage persists regardless of how security practices or technologies evolve.

Context Matters More Than Expertise

Champions' most valuable contribution isn't necessarily deep security expertise. It's combining reasonable security knowledge with deep understanding of their teams' contexts, constraints, and priorities.

A champion who understands their team's business requirements and can translate security concerns into that context provides more value than a security expert who lacks that contextual understanding. This principle remains true even as technical demands on champions increase.

Trust Enables Security

Security that depends primarily on control and enforcement is brittle and resisted. Security that's built on trust and collaboration is robust and embraced. Champions build the trust relationships that enable effective security collaboration.

These trust relationships develop through human connection, demonstrated competence, and genuine partnership. That human foundation for effective security won't be automated away.

(Illustration suggestion: A diagram showing "Enduring Principles" at the centre (People, Distributed Capability, Context, Trust) with

"Evolving Practices" around the outside (Automation, Remote Work, Threats, Tools) showing what changes and what remains constant)

Building for the Future

How do you build programmes that remain effective as circumstances evolve? Several principles guide future-oriented programme design.

Stay Flexible

Don't build programme structures that assume current circumstances will persist. Technology will change. Threats will evolve. Organisational practices will shift. Programmes designed with rigid assumptions about how work happens or what capabilities champions need quickly become obsolete.

Build flexibility into your programme. Focus on principles and outcomes rather than specific processes. Create structures that can adapt as circumstances change. Don't over-optimise for current reality at the expense of future adaptability.

Invest in Fundamentals

Trends come and go. Specific tools and practices become obsolete. But fundamental capabilities remain valuable across changing circumstances.

Critical thinking and problem-solving. Communication and influence. Learning agility and adaptability. Relationship building and collaboration. These fundamental capabilities serve champions well regardless of how specific security practices evolve.

Invest heavily in developing these fundamentals alongside technical security knowledge. Champions with strong fundamentals can adapt to new tools, threats, and practices. Champions with only specific technical knowledge struggle when those specific technologies change.

Watch for Weak Signals

Future changes often announce themselves through weak signals before they become obvious trends. The champion who's struggling with remote collaboration tools. The team is experimenting with new AI capabilities that raise novel security questions. The regulatory change in one jurisdiction might spread.

Pay attention to these weak signals. They indicate where your programme might need to evolve before the need becomes urgent. Early adaptation is easier than responding to a crisis.

Emma proactively monitors trends: *"I talk regularly with champions about emerging challenges they're facing. I follow discussions in the security industry about new threats and practices. I watch what*

regulatory changes are happening globally, even if they don't immediately affect us. These inputs help me spot trends early so we can evolve our programme proactively rather than reactively. We've adapted to several emerging needs before they became critical because we saw weak signals and responded early."

Experiment Continuously

Don't assume your current programme design is optimal. Experiment with new approaches. Test different training methods. Try alternative engagement models. Explore emerging tools and practices.

Make experimentation safe by testing with small groups before implementing broadly. Learn from experiments that fail as well as those that succeed. Create a culture where trying new approaches is valued even when they don't all work out.

This experimental mindset keeps programmes fresh and evolving whilst preventing stagnation.

A Note on Uncertainty

Predicting the future is inherently uncertain. Some trends discussed in this chapter will accelerate. Others will prove less significant than they appear. Completely unexpected developments will emerge, reshaping champions programmes in ways we can't anticipate.

That uncertainty is fine. You don't need perfect foresight to build effective programmes. You need awareness of current trends, flexibility to adapt as circumstances change, investment in fundamentals that remain valuable across scenarios, and willingness to experiment and evolve.

The programmes that thrive over the next decade won't be those that perfectly predicted the future. There will be those who built strong foundations, maintained flexibility, responded thoughtfully to emerging changes, and focused relentlessly on the core purpose of enabling effective security through distributed capability.

The Enduring Value

Despite all the changes and uncertainties, one thing remains clear: the fundamental value proposition of Security Champions programmes is sound and likely to become more valuable, not less.

Organisations need security capability distributed throughout their technology teams, not concentrated solely in central security teams. They need security thinking integrated into daily work, not imposed through external review processes. They need people who combine technical capability with security awareness and who are positioned where decisions are made.

Security Champions programmes provide these capabilities. As organisations grow, as technology complexity increases, and as security threats evolve, the need for distributed security capability intensifies rather than diminishes.

The specific practices will evolve. The tools will change. The threats will shift. But the core need for people who can bring security thinking to their teams, whilst building security culture and bridging between security specialists and development teams, will remain.

David, who's built and sustained a programme for five years, reflects on this: "I've watched our programme evolve substantially. How we train champions has changed. What tools champions use have changed. What threats we focus on has changed. But the fundamental value of having security-capable people embedded in development teams hasn't changed. If anything, it's become more obvious and more essential as our organisation has grown and our security challenges have become more complex."

Your Role in This Evolution

If you're building or running a Security Champions programme, you're helping shape how these programmes evolve. The innovations you develop, the lessons you learn, and the approaches

you test contribute to the collective wisdom about what makes champion programmes effective.

Share your experiences with the broader community. Publish case studies. Present at conferences. Participate in practitioner forums. The field benefits when programme leaders learn from each other's successes and failures.

Experiment boldly whilst measuring thoughtfully. Try new approaches but assess whether they actually improve outcomes. Not every innovation works, but we only discover what works through experimentation.

Stay connected to practitioners in other organisations. The challenges you face aren't unique. Other programme leaders are navigating similar issues and developing solutions you can learn from.

Build programmes that survive beyond your involvement. Document your thinking. Develop other leaders. Create resilient structures that can evolve without depending on you personally. Your legacy isn't just a successful programme during your tenure, but one that continues to thrive after you move on.

Final Thoughts

Security Champions programmes represent a fundamental shift in how organisations approach security. Rather than viewing security as solely the responsibility of security specialists, they recognise that effective security requires capability distributed throughout the organisation. Rather than imposing security through external control, they build security into how teams think and work.

This shift isn't easy. It requires sustained investment, thoughtful design, patient culture change, and continuous adaptation. But the organisations that make this shift successfully achieve security outcomes that centralised approaches alone can't deliver.

The future will bring changes we can't fully predict. New threats, new technologies, new practices, new challenges. But the organisations that have invested in building strong Security Champions programmes will be well-positioned to navigate those changes effectively.

Because ultimately, security isn't about tools or processes or technologies. It's about people making good decisions under uncertainty and time pressure. It's about cultures where security is valued and enabled. It's about organisations where security thinking is distributed throughout rather than concentrated in isolated teams.

Security Champions programmes build that distributed capability, that security culture, that organisational resilience. That mission will remain relevant and valuable regardless of how the specifics evolve.

If you're building such a programme, you're doing important work. Work that protects your organisation, develops people's capabilities, and influences organisational culture. Work that will deliver compounding value over time as capabilities mature and culture shifts.

The journey is challenging. But it's worth it.

Thank you for your time and patience in reading this book. I hope it has been informative and has helped you understand the real power of Security Champions and what they can achieve for you and your organisation.

All the best.

Appendix: 90-Day Programme Launch Plan

This plan provides a structured approach to launching your Security Champions programme during the critical first 90 days.

Pre-Launch (Weeks -4 to 0)

Week -4: Foundation Setting

- Secure executive sponsorship and alignment
- Define programme vision, goals, and scope
- Identify initial champion recruitment targets (8-12 for first cohort)
- Establish basic programme structure and governance

Week -3: Stakeholder Engagement

- Meet with key stakeholders to explain the programme and secure support
- Identify potential champions through manager nominations and self-nominations
- Begin recruiting initial champion cohort
- Set up communication channels (Slack, Teams, etc.)

Week -2: Champion Selection

- Conduct recruitment conversations with prospective champions
- Confirm champion commitment and manager support
- Finalise initial cohort (aim for 8-12 champions)
- Schedule launch activities

Week -1: Launch Preparation

- Prepare onboarding materials and initial training content
- Set up programme infrastructure (channels, documentation, meeting schedules)
- Communicate launch to broader organisation
- Finalise logistics for first champion session

Month 1: Launch and Onboarding

Week 1: Kick-off

- Champion kick-off session (2-3 hours)
- Programme vision and goals
- Role expectations and boundaries
- Introduction to the security team
- Initial community building

- Pair each new champion with an experienced security team member or (if available) an existing champion
- Establish weekly check-in rhythm

Week 2: Foundation Building

- First focused training session on your organisation's most common security issues
- Champions begin engaging in their team activities with a security lens
- Office hours available for champion questions
- Individual check-ins with each champion

Week 3: Practical Application

- Second training session on practical security reviews in your technology stack
- Champions conduct first security activities (guided reviews, design participation)
- Community discussion: early experiences and questions
- Continue individual support

Week 4: Early Wins

- Celebrate early champion contributions (even small ones)
- Third training session on a specific security domain

- Champions begin answering basic team security questions
- End-of-month retrospective with champions

Month 2: Capability Development

Week 5-6: Deepening Expertise

- Training on threat modelling basics
- Champions participate in actual threat modelling exercises
- Increase champion independence in security decisions
- Continue weekly office hours and community engagement

Week 7-8: Expanding Scope

- Training on secure coding practices specific to your stack
- Champions begin proactive security contributions (not just reactive)
- First measurement of early impact
- Mid-programme check-in with each champion

Month 3: Establishing Rhythm

Week 9-10: Consolidation

- Review what's working and what needs adjustment
- Refine programme elements based on feedback

- Champions handling most routine security questions independently
- Begin documenting common security patterns and decisions

Week 11-12: Looking Forward

- 90-day retrospective with champions
- Measure and communicate early impact to stakeholders
- Plan for second cohort recruitment (if expanding)
- Establish sustainable ongoing rhythm

Key Success Indicators at 90 Days

Champion Engagement

80%+ of initial champions are still actively engaged

Regular participation in community discussions

Champions handling security questions in their teams

Capability Development

Champions can identify common security issues in your stack

Champions know when and how to escalate appropriately

Champions providing value to their teams (validated by team feedback)

Programme Health

Clear programme structure and processes
Sustainable support model established
Positive champion satisfaction (validated by survey or conversations)
Early security impact visible (issues caught earlier, teams asking more security questions)

Common Pitfalls in the First 90 Days

Moving Too Fast

Trying to recruit too many champions or cover too much content. Better to start small and build a strong foundation.

Insufficient Support

Underestimating the support champions need initially. Plan for intensive support in the first months.

Unclear Expectations

Not being explicit about what champions do and don't do. Clarity prevents frustration.

Measurement Overload

Trying to measure everything perfectly from day one. Start with basic health indicators, and expand measurement over time.

Neglecting Community

Focusing only on training without building champion relationships and community. Community sustains engagement long-term.

A Personal Request from the Author

If you found this book helpful, inspiring, or thought-provoking, I'd be incredibly grateful if you could take a few moments to leave a review on the platform where you purchased it. Your feedback doesn't just help others discover the book - it also plays a vital role in supporting the broader mission of spreading cyber wisdom to more homes, schools, and communities.

Every review makes a difference, and your words will help this topic reach those who need it most.

Beyond this book

Security Champions are at the forefront of applying behavioural science to foster a culture of cybersecurity. To stay ahead with the latest theories, models, and practices - and to access whitepapers, guides, and tools tailored to empowering Security Champions - visit our Champions page at https://CyBehave.com/champions.php