SECURITY LEADERSHIP SERIES

The CISO First 90 Days Playbook

A structured framework for security leaders taking on a new role.

Three phases — understand and baseline, design and align, deliver and demonstrate — with the diagnostics, conversations and outputs that make each one land.

Mark R. Watts BSc CISSP CISM

Contents

Introduction

A role-agnostic first 90 days framework for any incoming CISO, Head of Cyber Security, or equivalent security leader. Structured around three overlapping phases: understand and baseline, design and align, and deliver and demonstrate, and informed by Michael D. Watkins' *The First 90 Days*, in particular the STARS model, the five conversations with your new boss, and the discipline of securing early wins.

This playbook works alongside four companion templates included in this pack: the STARS Diagnostic Worksheet, the Five Conversations Tracker, the 30/60/90 Outputs Checklist, and the Stakeholder Map Template. Use the diagnostic worksheet first, since it shapes how you apply everything that follows.

Why 90 Days Matters

Watkins' central argument is that leadership transitions are periods of acute vulnerability and acute opportunity. Every new leader starts as a net consumer of value and only later becomes a net contributor. Watkins calls the crossover the **breakeven point,** and his research puts the average at roughly six months into a new role. The purpose of a deliberate 90-day plan is to pull that breakeven point forward: build momentum early, avoid the vicious cycles that trap new leaders, and establish credibility before the organisation's patience runs out.

For a CISO this is sharpened by the nature of the role. Security leaders inherit live risk from day one; an incident in week two does not wait for the strategy to be written. The plan therefore has to balance structured learning with a minimum viable operational grip from the outset.

Common Transition Traps for a New CISO

Watkins catalogues the classic failure modes of new leaders. Translated into security terms:

> **Sticking with what you know.** Rebuilding your last organisation's security programme in the new one, regardless of fit. What worked in a bank may be wrong for a charity, a scale-up, or a university.

> **The action imperative.** Feeling compelled to make visible technical changes before understanding the environment. Buying tooling in month one is the CISO version of this trap.

> **Coming in with "the answer."** Announcing conclusions before doing the diagnosis. Even if the answer turns out to be right, the organisation resents not being consulted, and adoption suffers.

> **Attempting too much.** Launching a dozen workstreams and finishing none. Better three visible, completed improvements than a sprawling programme with nothing landed.

> **Neglecting horizontal relationships.** Optimising for the boss and the team while ignoring peers: Legal, HR, Data Protection, Finance, and the business unit leaders whose cooperation every control ultimately depends on.

> **Undefended boundaries.** Accepting every inherited commitment and every new request. If you do not negotiate expectations early, others will define your role for you.

Diagnose the Situation First: the STARS Model

Watkins' STARS framework is the pivot of the whole book: **match your strategy to the situation**, because the right approach in one context is actively harmful in another. Diagnose which situation, or blend, since most real roles are a portfolio, you are walking into before committing to a plan. Use the STARS Diagnostic Worksheet in this pack to score your own situation against each dimension below.

STARS SITUATION	WHAT IT LOOKS LIKE	WHAT IT DEMANDS	WATCH-OUTS
Start-up	Greenfield build: no existing security function, no strategy, no team.	Assemble capability from scratch: strategy, operating model, first hires, foundational controls.	No existing structures to lean on. Risk of exhaustion from building all fronts at once; sequence ruthlessly.
Turnaround	Post-breach recovery, a failed audit, or a security function widely acknowledged to be broken.	Fast, decisive action. Stabilise, triage, cut what is not working, make hard calls early.	The "hunkering in the bunker" risk. Decisive does not mean reckless; a wrong early call is highly visible.
Accelerated growth	Security must scale with the organisation: headcount doubling, new markets, new regulatory exposure.	Put structures and repeatable systems in place without strangling the growth that pays for them.	Growth hides debt. Controls that coped at 200 staff fail silently at 800.
Realignment	A security function that has drifted: stale policies, shelfware tooling, compliance theatre.	Convince people change is needed at all. Build the case with evidence before proposing the cure.	Charging in like a turnaround alienates people who believe things are fine.
Sustaining success	Inheriting a mature, well-regarded security programme from a strong predecessor.	Preserve what works, understand why it works, and find the next level.	Living in the predecessor's shadow. Success here is quieter and slower to demonstrate.

Most CISO roles are a blend. For example, a start-up build (no team) inside a realignment context (an organisation that does not yet believe it needs one). Diagnose each dimension separately: the team, the tooling, the governance, and the culture may each sit in a different STARS quadrant, and each needs a matched approach.

Negotiate Success: The Five Conversations

Watkins argues the single most important relationship in a transition is with your new boss (for most CISOs the CIO, COO, CFO, or CEO), and that you should proactively structure five ongoing conversations rather than waiting for direction. Use the Five Conversations Tracker in this pack to prepare for and log each one.

1. **The situational diagnosis conversation.** Agree what kind of STARS situation this actually is. If you think it is a realignment and your boss thinks it is sustaining success, every subsequent disagreement flows from that gap.

2. **The expectations conversation.** What does good look like at 30, 60, 90 days and one year? Negotiate this explicitly, and revisit it as your diagnosis matures.

3. **The resources conversation.** Budget, headcount, political capital, and air cover. Link resources to outcomes: "with X I can deliver Y by Z."

4. **The style conversation.** How does your boss want to communicate: cadence, format, level of detail? What constitutes a "no surprises" escalation for security incidents?

5. **The personal development conversation.** Later in the transition: where do you need to grow, and what stretch does the role offer?

Days 1 to 30: Understand and Baseline

Watkins' first imperative is to **accelerate your learning**: treat learning as an investment with a defined agenda, not something that happens by osmosis. Arrive with hypotheses and a structured learning plan; leave the month with an evidence-based diagnosis.

PRIORITIES

- **Relationship-building first.** One-to-ones with your line manager, executive peers, the board or audit committee chair, Legal, Data Protection, HR, Finance, internal audit, and the leaders who own the most sensitive data and critical processes.
- **Listen before broadcasting.** Resist announcing a vision in week one. Early credibility comes from demonstrable listening and good questions, not from having the answer.
- **Technical and organisational baseline.** Asset and data inventory, architecture, current controls, identity posture, third-party landscape, incident history. Establish minimum viable incident response cover immediately.
- **Governance and reporting baseline.** Map how cyber risk currently reaches executive and board level, and the gap between that and a standing reporting line.
- **Regulatory and assurance context.** Position against relevant frameworks (NIST CSF, ISO 27001, Cyber Essentials, sector regulation), and open audit findings.
- **Run the STARS diagnosis and the first two conversations.**

OUTPUTS BY DAY 30

- Stakeholder map and engagement log
- Current-state risk and control baseline, framework-aligned
- Agreed STARS diagnosis and written expectations with your line manager
- Interim incident escalation arrangement in place
- Short briefing to your line manager on emerging priorities and any risks requiring immediate escalation

Days 31 to 60: Design and Align

This phase maps to Watkins' imperatives of **matching strategy to situation** and **achieving alignment:** ensuring strategy, structure, systems, and skills reinforce rather than fight each other.

PRIORITIES

- **Draft the security strategy.** Anchor it to a recognised framework and align it explicitly to the organisation's business and technology strategy. The strategy's tone should follow the STARS diagnosis.
- **Propose the target operating model.** Capability areas, a phased resourcing plan, and the build, buy, or partner case for capabilities such as 24/7 monitoring.
- **Quantify the top risks.** Bring risks into a consistent methodology (OpenFAIR or equivalent) so leadership sees risk in decision-useful terms.
- **Protect the crown jewels early.** Produce a focused risk assessment for the organisation's most sensitive estate ahead of the wider strategy being finalised.
- **Create alliances.** Identify who must support the strategy at approval, and invest in the persuadables now.
- **Start the security culture work.** Early engagement models with delivery teams rather than late-stage compliance gates.

OUTPUTS BY DAY 60

- Draft security strategy and target operating model, pre-socialised with key stakeholders
- Quantified top-10 risk register
- Resourcing and investment business case
- Crown-jewels risk assessment (interim)
- Team assessment complete, with any role or people changes identified

Days 61 to 90: Deliver and Demonstrate

Watkins' **secure early wins** imperative governs this phase. Early wins should be chosen deliberately: matters that your key stakeholders care about, achievable within the window, defensible as the right thing, and introduced in a way that models the culture you want the function to be known for.

PRIORITIES

- **Secure formal approval** for the strategy and operating model at the appropriate executive or board forum.
- **Land one or two visible early wins.** Completed and communicated beats broad and unfinished.
- **Establish the standing governance rhythm.** First periodic risk report, incident response plan tested at least on paper, third-party risk process started.
- **Begin recruitment** against the agreed structure.
- **Keep your balance.** A CISO who burns out at day 80 delivers none of the above; sustainable pace is a professional obligation, not a luxury.

OUTPUTS BY DAY 90

- Approved security strategy and operating model
- At least one delivered, visible, communicated security improvement
- Standing risk reporting cadence in place
- Recruitment underway for the first hire(s)
- A credible, evidenced 90-day narrative for the next leadership update

Key Relationships to Prioritise

STAKEHOLDER	WHY IT MATTERS EARLY
Line manager (CIO, COO, CFO, or CEO)	The five conversations run through this relationship; expectations, resources, and the STARS diagnosis are agreed here.
Executive board, board, or audit and risk committee	Formal sponsors of strategy and investment; the audience for the standing risk reporting line.
Owners of the most sensitive data and critical processes	The crown-jewels estate; where the first focused risk work and the most valuable alliances sit.
Data Protection and Legal	Regulatory obligations sit close to all security work; early alignment prevents later conflict.
HR	Team assessment, recruitment, insider risk, and the people dimension of security culture.
Finance	The investment case lives or dies on a relationship built before the case is submitted.
Internal audit	Existing findings are a ready-made evidence base and a source of early-win candidates.
Peer business unit leaders	The horizontal relationships whose cooperation every control ultimately depends on.

Risks and Watch-Outs

- **Misdiagnosing the STARS situation,** treating a realignment like a turnaround or a turnaround like sustaining success.
- **Skipping the expectations conversation,** letting success criteria stay implicit, then discovering at day 90 that your boss was measuring something else.
- **The action imperative and premature tooling purchases,** visible activity substituting for diagnosis.
- **Over-indexing on technical delivery at the expense of relationships,** the strategy that fails at approval usually failed weeks earlier in the corridors.
- **Inherited commitments,** audit responses, supplier contracts, and programme promises made before your arrival.
- **An incident before the plan is ready,** hence the interim escalation arrangement in month one.
- **Attempting too much,** protect the shortlist of early wins from the temptation to fix everything at once.

THE ONE-LINE TEST AT DAY 90

Can you tell a credible, evidenced story — what you found, what you fixed, what comes next — that your boss, your board, and your team would all recognise as true? If yes, the breakeven point is moving in the right direction.

Companion Templates

This playbook is designed to be used alongside four companion templates, provided as a separate editable workbook:

STARS Diagnostic Worksheet Score your own situation across team, tooling, governance, and culture.	**Five Conversations Tracker** Prepare for and log each conversation with your line manager.
30/60/90 Outputs Checklist A tickable tracker for every output named in this playbook.	**Stakeholder Map Template** Build your relationship map, engagement log, and approval alliance map.

THE CISO FIRST 90 DAYS PLAYBOOK

Mark Watts

Security leadership advisory, interim CISO engagements, and transition support for organisations appointing a new head of cyber security.

markrwatts.com

The STARS model, the five conversations, and the breakeven point are concepts drawn from *The First 90 Days* by Michael D. Watkins (Harvard Business Review Press); they are referenced and applied here for security leadership, not reproduced.

EDITION 1.0 · PLAYBOOK + 4 COMPANION TEMPLATES