



THE CISO CRUCIBLE

THE NEW CISO FIELD GUIDE

Your first 90 days, from an inherited mess to a program that runs without you.

*Every CISO builds a plan.
The ones who survive treat it as a compass, not a
map — and keep asking one question: **am I making
progress, or am I just busy?***

Drawn from the novel *The CISO Crucible* by Andy Dyrz
Sterling Security Press · thecisocrucible.com

The Core Lesson

William Sterling walked into BigCo with a 90-day plan. It didn't survive Day 1. That's not a failure story — it's the point. Every CISO builds a plan; the ones who succeed treat it as a compass, not a map. This guide gives you progress markers you can check no matter what crises have rearranged your calendar.

*One question drives everything: **Am I making progress, or am I just busy?***

IF YOU DO NOTHING ELSE

Quick-Start: Your First Five Actions

Do these five things in your first week.

- 1 Start a Delay Log.** Every time a decision needs cross-departmental permission, write it down: date, decision, who you needed, how long it took. This one document becomes your most powerful evidence at Day 30.
- 2 Run 1-on-1s with every direct report.** Don't ask "what's broken." Ask "what would you fix if you had air cover?" The gap between those answers reveals your team's trust level.
- 3 Inventory shadow AI usage.** Send a brief, non-threatening survey to department heads. Assume the real number is 3x what they report. Know the actual attack surface before you defend it.
- 4 Learn why your predecessor failed.** Request the exit interview, talk to the people who worked with them, read between the lines. The fault lines that broke them will try to break you.
- 5 Identify who was passed over for your role.** Ask HR, ask your boss, ask whoever recruited you. These people are future allies or active threats — know which before your first all-hands.

1

DAYS 1-30

Get the Lay of the Land

Orientation under fire. You walk into someone else's mess: listen, observe, map the politics, and survive your first board meetings and inherited incidents. You're building situational awareness while everything around you says you should be acting. Resist.

Before Day 1 • Preparation

- ☐ **Learn why your predecessor failed** — request the exit interview, read between the lines, and identify the political fault lines that broke them before they break you. CH 2
- ☐ **Identify who felt passed over for your role** — ask HR, your new boss, the person who recruited you. These people shape your political landscape from minute one. CH 2
- ☐ **Draft your 90-day plan, then hold it loosely** — you need a compass, not a map. Write it down so you can measure deviation, not follow it blindly. CH 1
- ☐ **Know your actual timeline** — not the one you planned, the one the organization already committed to regulators, partners, and the board. Your deadline may already be set. CH 2
- ☐ **Research the regulatory landscape** — what filings are pending? What audits are scheduled? What did the last regulator communication say? These shape your real timeline. CH 2, 11

Days 1–5 • Orientation Under Fire

- ☐ **Start a Delay Log** — document every decision that required cross-departmental permission: date, decision, who you needed, wait time. CH 1
- ☐ **Document reporting-structure bottlenecks** — map who reports to whom, where security sits, and every place your authority doesn't match your accountability. CH 3
- ☐ **Conduct 1-on-1s with every direct report** — ask "what would you fix if you had air cover?" not "what's broken?" CH 3
- ☐ **Inventory shadow AI usage** — a brief, non-threatening survey to department heads. Assume the real number is 3x what they report. CH 2
- ☐ **Map who's documenting your decisions** — someone is already building a file. Identify them early and give them nothing to weaponize. CH 4
- ☐ **Respond to every outreach from former employees** — institutional knowledge left with them. The ones reaching out are telling you something. CH 3
- ☐ **Write down what confuses you every evening** — the pattern hiding in your confusion is the framework you'll need later. CH 1, 7
- ☐ **Identify your team's unspoken fears** — listen for what wounded teams aren't saying. Silence is data. CH 3
- ☐ **Protect different working styles immediately** — if your best analyst has a "Do Not Disturb" sign, don't override it. Their focus is your detection capability. CH 4
- ☐ **Separate the confidence you perform from the uncertainty you manage** — your team needs steadiness; your journal needs honesty. CH 2

CHECKPOINT

Day 5 Self-Assessment

On track if you answer YES to at least four:

- ☐ I know why the last person in this role failed or left
- ☐ I've spoken 1-on-1 with every direct report
- ☐ I have a written list of at least three authority/accountability mismatches
- ☐ I know who felt passed over for my role and have assessed their posture
- ☐ I've started my Delay Log and have entries in it
- ☐ I can name the top three things my team is afraid to tell me

WARNING SIGNS

- ◇ You've made promises about what you'll fix (not enough data yet)
- ◇ You've reorganized anything (it's Day 5)
- ◇ You skipped 1-on-1s because a crisis pulled you in

Days 6–14 • Mapping the Terrain

Now you can ask harder questions — but you're still in discovery mode, not fix-it mode.

- ☐ **Run a full shadow IT audit** — every SaaS subscription, personal device, and workaround someone built because the official tool didn't work. One SaaS purchase can mean 50+ accounts and separate attack vectors. CH 3, 6
- ☐ **Map data flows to every external service** — APIs, integrations, vendor connections. The volume will be worse than you expect. CH 6
- ☐ **Audit pages 40–150 of every major vendor contract** — that's where AI training rights, data-usage clauses, and liability limits hide. CH 17
- ☐ **Assume your IP is already in AI training models** — check which tools have been feeding company data to external models. CH 6
- ☐ **Check physical security basics** — walk the building. Broken badge readers, propped doors, unlocked server rooms. Broken locks indicate broken culture. CH 6
- ☐ **Accept that shadow IT exists and govern it** — banning drives it underground; governing brings it into visibility. CH 6
- ☐ **Initiate threat hunting** — don't wait for alerts. Assume persistent threats are present and task your best analyst to go looking. CH 4
- ☐ **Create clean enclaves for business continuity** — identify systems you can isolate during IR so the business keeps running while you contain threats. CH 4
- ☐ **Map the political landscape** — lunch patterns, meeting invitations, who gets cc'd. Identify the real decision-makers. CH 7
- ☐ **Give territorial leaders partnership roles** — invite IT Ops, Engineering, and Infrastructure to co-own security outcomes. Partnership, not subordination. CH 4
- ☐ **Calculate per-hour business impact of downtime** — get finance to validate the number. This one figure changes every board, insurance, and vendor conversation. CH 5
- ☐ **Accept that your company contains multiple incompatible cultures** — the engineering floor and the sales floor are different countries. Stop trying to unify them. CH 7
- ☐ **Observe three times longer than feels comfortable before acting** — in stakeholder relationships, premature action costs more than delayed action. CH 7

Days 15–30 • Building Your Case

You've seen enough to know what's wrong. Now build the evidence to prove it.

- ☐ **Identify every single point of failure — human and technical** — if one person's absence would cripple a function, that's your most urgent problem. CH 8
- ☐ **Build redundancy plans before your heroes break** — and they will. Cross-train now, not after the 2am call that doesn't get answered. CH 8
- ☐ **Document what's not working before you understand why** — you don't need root cause to justify action on single points of failure. CH 8
- ☐ **Establish DDoS mitigation and IR vendor relationships** — sign the contracts and run a tabletop. When the crisis hits, procurement paperwork is not an acceptable delay. CH 5
- ☐ **Design graduated response plans** — not every incident is a five-alarm fire. Build playbooks that show progress without full mobilization. CH 5
- ☐ **Order a real penetration test** — not a compliance checkbox, an actual adversary simulation. Test security, not compliance. CH 9
- ☐ **Document every authority/accountability mismatch formally** — specific examples, specific consequences. This becomes your most powerful board slide. CH 9
- ☐ **When smart people hint you're missing something, believe them** — your team sees what you can't. Hesitation is signal, not noise. CH 9
- ☐ **Disclose known problems to the board before regulators find them** — you earn trust by volunteering bad news and lose it permanently when they hear it elsewhere. CH 11
- ☐ **Map every regulator's unique requirements** — they don't coordinate. Build a matrix of who wants what, in what format, on what timeline. CH 11
- ☐ **Fight for structural changes during crisis** — when evidence is undeniable, the reorg conversation becomes possible. Use your Delay Log. CH 11
- ☐ **Build direct board relationships** — don't let IT monopolize executive communication. Get your own seat at that table. CH 11

CHECKPOINT

Day 30 Self-Assessment

On track if you answer YES to at least five:

- ☐ I have a complete asset inventory (including shadow IT) — even if it's ugly
- ☐ I've presented to the board at least once and they know the real state of security
- ☐ I have written documentation of every human single point of failure
- ☐ I've established at least one external IR/mitigation vendor relationship
- ☐ My Delay Log has enough entries to justify structural changes
- ☐ I can articulate per-hour business impact of a major outage in dollars
- ☐ At least one leader who opposed me now considers me a partner
- ☐ My team has told me something they were afraid to tell my predecessor

WARNING SIGNS

- ◇ You still can't name the shadow IT tools in use
- ◇ The board hasn't heard bad news from you yet
- ◇ Your best people are working late every night and you haven't addressed it
- ◇ You've been so deep in crises you haven't built relationships with business leaders

Build the Foundation

Turn observation into structure. This is where most new CISOs fail: the methodology that worked at your last company isn't working here. The question is whether you can see it — and adapt.

The Framework Diagnostic

Before implementing anything new, ask three questions about every department you're trying to secure.

- 1 How do they make decisions?** Data and process, or relationships and consensus?
- 2 How do they build trust?** Track record and metrics, or shared experience and loyalty?
- 3 How do they measure success?** Quantitative targets, or qualitative outcomes and narrative?

These answers tell you whether you're dealing with a process-driven or a relationship-driven team. The same security message needs completely different packaging for each.

If the answer is data / metrics / process...	If the answer is relationships / narrative / consensus...
Lead with spreadsheets, ROI models, and compliance frameworks	Lead with stories, mission alignment, and collaborative design
Provide documented procedures and clear success criteria	Provide vision, invite co-creation, and celebrate contributions
<i>Your CFO wants risk-adjusted returns on every control</i>	<i>Your creative team wants to know how security protects their mission</i>

Adapt Your Approach

- ☐ **Watch for the quiet breakdown** — monitor workload on your strongest contributors. If someone hasn't taken a day off in three weeks, intervene before they shatter. CH 12
- ☐ **When the same approach fails everywhere for different reasons, examine the approach** — the problem isn't the teams; it's the assumption that one method fits all. CH 8, 12
- ☐ **Know the human cost you're willing to accept before you push** — decide this in advance, not in the aftermath of a breakdown. CH 12
- ☐ **Test frameworks gradually** — full rollout can destroy organizations. Pilot, learn, adapt, expand. CH 12
- ☐ **Map every department's communication DNA** using the three diagnostic questions above. CH 14
- ☐ **Develop two versions of every initiative** — same objective, different delivery. Metrics and ROI for finance; narrative and mission for the creative teams. CH 14, 15
- ☐ **Find your translators** — people fluent in both relationship-driven and process-driven communication. Formalize them as security liaisons. CH 14
- ☐ **Protect individuals whose style doesn't match their department** — build roles that fit how they actually work. CH 14
- ☐ **Identify workarounds that are actually successful translations** — someone has already made security work for their team. Find them and learn. CH 15
- ☐ **Test new approaches quietly before announcing** — pilot with a willing team; let results speak before you ask for buy-in. CH 15
- ☐ **Ask for partnership, don't announce programs** — "We'd like your help designing this" converts ten times more people than "Here's what we're rolling out." CH 15
- ☐ **Catch yourself falling into old patterns** — your last company's playbook is your comfort zone, not your best option. Adjust mid-conversation. CH 15
- ☐ **Build your CFO alliance through data** — model each control as an investment with risk-adjusted returns. Spreadsheets, not coffee. CH 16
- ☐ **Position security spending as an investment portfolio** — risk-adjusted returns, not cost justification. CH 16
- ☐ **Use insurance negotiations as external validation** — the carrier's actuarial requirements independently prove what you've argued. CH 16
- ☐ **Audit and renegotiate vendor contracts** — map all vendor data flows. Your IP is leaking through APIs you forgot existed. CH 17
- ☐ **Build vendor risk scoring with real consequences** — a score without an action trigger at each level is theater. CH 17
- ☐ **Use crisis leverage to force vendor transparency** — vendors are most cooperative after they've failed you. Don't waste the moment. CH 17
- ☐ **Convert vendor governance into competitive advantage** — customers value partners who govern their supply chain. CH 17

CHECKPOINT

Day 60 Self-Assessment

On track if you answer YES to at least five:

- ☐ I can describe every major department's communication style without the word "resistant"
- ☐ I've adapted my delivery for at least two teams and seen better engagement
- ☐ I have a financial model that frames security spending as investment, not cost
- ☐ No one on my team is in a burnout danger zone — and I'd know if they were
- ☐ I've piloted at least one initiative with a willing team before rolling it out
- ☐ I have at least one unexpected ally — someone who opposed me early and now champions security
- ☐ My vendor risk framework has defined consequences, not just scores
- ☐ I've been to the board twice and the conversation is getting more strategic

WARNING SIGNS

- ◇ Every department still calls security "the team that says no"
- ◇ You're still using one playbook for every audience
- ◇ Your strongest team member is exhausted and you're rationalizing it
- ◇ Your CFO still sees security as pure cost

3 DAYS 61-90

Validate and Gain Momentum

The program gets tested under real pressure — attacks, regulators, vendors, and the board all converge. The final test isn't whether you can run security. It's whether security runs when you step back.

Prove the System Works Without You

- ☐ **Launch a champion program and let champions self-select** — forced participation fails. Natural leaders know their terrain better than you do. CH 18
- ☐ **Gamify security engagement** — leaderboards, badges, public recognition turn compliance into competition. CH 18
- ☐ **Trust distributed intelligence over centralized control** — ten empowered champions outperform one exhausted security team. CH 18
- ☐ **Enable different champion types for different departments** — a champion in Engineering looks different from one in Marketing. Let the role adapt. CH 18
- ☐ **Separate your strategic role from operational execution** — build a CISO + Head of Security Ops model so the machine doesn't need you for every decision. CH 18
- ☐ **Build behavioral baselines for all executives** — document communication patterns and quirks. They become your detection signatures against impersonation and deepfakes. CH 19
- ☐ **Train champions on communication pattern recognition** — social engineering exploits human patterns. Your champions are your early-warning system. CH 19
- ☐ **Document executive quirks as security signatures** — the CEO who never texts; the CFO's stock phrases. Deviations from pattern are your alerts. CH 19
- ☐ **Map every bitter departure to a potential attack vector** — former employees with grudges know your systems intimately. CH 21
- ☐ **Build rotation schedules before the next crisis** — if you're building the schedule during the crisis, you're already too late. CH 21
- ☐ **Design your crisis response to function without you — then test it** — the real validation is when your team handles an incident and you hear about it afterward. CH 21
- ☐ **Track response-time improvement across incidents** — if your second major incident isn't handled faster than the first, your systems aren't learning. CH 21
- ☐ **Lead your board presentation with ROI in business language** — revenue enabled, losses prevented, advantage created. Technical detail goes in the appendix. CH 22
- ☐ **Prepare for "why did we still have losses"** — reframe every incident as validation of resilience. The goal was never zero incidents; it was fast recovery. CH 22
- ☐ **Show customers real crisis management** — prospects care more about how you handle problems than whether you claim to have none. CH 20
- ☐ **Architecture beats obscurity** — ensure critical backups are immutable, not just hidden. CH 20
- ☐ **Focus on recovery time as your primary metric** — prevention is unverifiable; recovery is measurable. CH 20
- ☐ **Trust enables discovery** — people reveal hidden systems and workarounds when they trust you won't punish them. This is your ongoing asset-discovery program. CH 20
- ☐ **Prove profit-center status with revenue AND savings** — show the deals that closed because of security, not just costs reduced. CH 22
- ☐ **Schedule post-incident analysis 48+ hours after resolution** — exhausted teams find blame; rested teams find insights. CH 21
- ☐ **Finish with margin** — professionals complete before deadlines, not on them. CH 22

CHECKPOINT

Day 90 Self-Assessment

On track if you answer YES to at least five:

- ☐ My team handled at least one incident without me directing the response
- ☐ I have champion volunteers in at least three departments outside security
- ☐ The board discusses security as a business function, not a cost center
- ☐ I can show measurable improvement in response times across incidents
- ☐ My financial case includes revenue enabled, not just losses prevented
- ☐ At least one deal explicitly cited security posture as a factor
- ☐ I have a succession plan — someone can cover my role for two weeks unnoticed
- ☐ I spent more time this week on strategy than on firefighting

COURSE-CORRECT IF

- ◇ You're still the bottleneck for incident decisions
- ◇ "Security champion" is an assigned duty, not a volunteer role
- ◇ The board still asks "are we secure?" instead of "what's our risk posture?"
- ◇ You can't point to revenue that security helped create

Beyond Day 90 • Ongoing Health Checks

QUARTERLY

Ongoing Self-Assessment

- ☐ Have I built any new cross-departmental relationships this quarter?
- ☐ Is my team's average response time still improving?
- ☐ Can I name three worries my team has that I've acted on?
- ☐ Has the board's security conversation moved beyond compliance checkboxes?
- ☐ Am I still adapting my communication for different audiences, or slipping back to one size?
- ☐ Is my champion program growing organically, or have I stopped investing in it?
- ☐ Could my team handle a crisis this week without me? (If you're not sure, the answer is no.)

The Diagnostic Toolkit

Four templates you can use from Day 1. Editable versions (.xlsx) are at thecisocrucible.com/fieldguide.

The Delay Log

Keep this running from Day 1. It becomes your most powerful evidence for structural change.

Date	Decision Needed	Who I Needed	Wait Time	Impact of Delay	Resolution
e.g.	Approve IR vendor contract	Legal, Procurement, CFO	11 days	No IR capability during a Week 2 incident	Emergency sign-off after incident

Stakeholder Communication Map

Stakeholder	Decision Style	Trust Currency	Success Metric	Best Security Framing
CFO	Data-driven, process	Track record, accuracy	ROI, risk reduction %	Investment-portfolio model
Creative Director	Relationship, narrative	Shared vision, loyalty	Mission impact, morale	"How this protects your team's work"

Single Point of Failure Register

If the "Backup Plan" column is empty, that's your first action item.

Function	Person / System	Backup Plan	Status	Last Tested
Malware analysis	Senior analyst (solo)	Cross-train 2 juniors	In progress	Not yet tested

Vendor Risk Scorecard

A score without a defined consequence is theater.

Vendor	Data Access	Contract Reviewed?	Risk Score	Consequence at This Score	Last Review
Cloud provider	Full customer data	Yes — AI clause found	High	Renegotiate or migrate by Q2	2024-01-15

Topical Guides

Three of the leadership challenges the book returns to most often.

Board Communication for Security Leaders

The board doesn't speak your language. Neither does your CFO, or your digital-transformation team. But they all need to understand risk.

Translate risk into business impact

Security leaders lead with technical specificity: "We found 437 unpatched systems across 15 subnets." The board hears noise. Reframe: "We found systems that could give attackers access to customer payment data before we can detect them — a breach risk on our largest revenue stream. Here's what we're doing and what it costs."

- **The CFO** thinks in metrics — ROI, cost avoidance, financial impact. Show the downside: "A breach would cost \$X in remediation, fines, and lost trust. This investment prevents that."
- **The Board** thinks in narrative and accountability. Give them the story: where you were, where you're going, what's at stake if you don't get there.
- **Your Team** needs transparency and context — that you understand their constraints and the plan is realistic.

The structure that works

Every board presentation: **1.** Status quo (be honest — your predecessor may have oversold). **2.** What changed (new threats or capabilities, and the business impact). **3.** The plan (what you're doing, why it works, what success looks like in business terms). **4.** What you need (budget, headcount, structure — quantified). **5.** The alternative (what inaction costs — regulatory, breach probability, data loss).

The burnout warning *from The CISO Crucible*

You inherited a burned-out team, and that's a business risk, not just morale. Burned-out teams miss critical incidents and create process debt. Put team wellness in the board narrative: "We're investing in our team because operational security depends on people who can think clearly under pressure."

Building a Security Champion Program

The most common mistake new CISOs make is trying to be the security expert for every part of the company. You'll burn out, your team will burn out, and you'll create a culture where security is something done *to* departments, not *with* them.

Distribute ownership

A champion program inverts this. Identify leaders in each function — product, sales, engineering, operations, finance — and make them responsible for security outcomes in their domain.

- **What champions do:** they're not security experts — they're business leaders who understand how security enables their area, and can make tradeoff decisions with context you don't have.
- **What champions get:** training (enough to understand the framework), air cover (you publicly back their security calls), and visibility (their contributions get recognized by their leadership).

- **What security provides:** guidance, tools, escalation paths, and accountability. You're the standard-setter, not the executor.

Why it works

When Jessica, the digital-transformation leader in *The CISO Crucible*, moved from opposing security to championing it, the dynamic changed entirely. She owned her business case, persuaded her peers, and moved faster because she didn't need sign-off on every detail. That's what a champion program creates: distributed decision-making that scales faster than any central team.

Getting started

1. Identify one or two potential champions — people with influence and credibility in their area.
2. Start small. Give them one concrete security outcome to own, not a whole function.
3. Make it visible. When they succeed, celebrate it publicly — security leadership is a career asset.
4. Iterate. Build the network over time; as they prove the model, others will want in.

The guiding principle *from The CISO Crucible*

"InfoSec doesn't need heroes — it needs systems." A champion program builds the system, so security is embedded in how decisions get made, not bolted on afterward.

Managing CISO Burnout and Team Wellness

Burnout isn't a personal weakness or low commitment. It's an organizational failure — the result of asking people to do impossible things without the resources, authority, or support to succeed.

Signs to watch for

In yourself: checking Slack at 11 PM and reading tickets before coffee; every decision feels career-ending; you've stopped thinking strategically because you're always firefighting; you're not sleeping well. **In your team:** people staying late and not taking vacation; the same person responding to every incident (a red flag, not excellence); mistakes increasing despite longer hours; new hires leaving within six months.

What to do about it

Immediate: make people take time off; rotate incident response so one person isn't the single point of failure; cut meetings so people can actually do the work. **Structural:** hire if you have fewer people than the work requires; automate the repetitive 20%; distribute work through a champion program.

The bottom line

A burned-out team misses critical events, makes mistakes under pressure, and leaves for competitors. Treating wellness as a security business problem — not an HR problem — is what good CISO leadership looks like.

Plans break. Trajectories don't have to.

Every item in this guide comes from *The CISO Crucible: A 90-Day Journey in Cybersecurity Leadership* — the meetings where these lessons were learned the hard way, the crises that forced the adaptation, and the relationships that made the difference.

Read Chapter 1 free and get the editable templates at thecisocrucible.com