CovertSwarm®

BURN THE RISK REGISTER

A CISO's First 90 Days

Why successful CISOs map the P&L before they map the network

Anders Reeves + Contributing CISOs

INTRODUCTION

Your predecessor likely left you a pristine Risk Register.

Burn it.

Perhaps not literally, though I've been tempted. The official Risk Register you've inherited is a compliance *artifact*, and in most cases not an operational *reality*. It's likely something your predecessor curated to make leadership comfortable, but not what's actually keeping the sysadmins awake at night.

I've held the CISO role before founding CovertSwarm, and since seen inside hundreds of organizations through our offensive security work. The pattern is clear: new CISOs who succeed in their first 90 days do things differently to the ones who struggle. It's not about working harder, it's about asking the right questions.

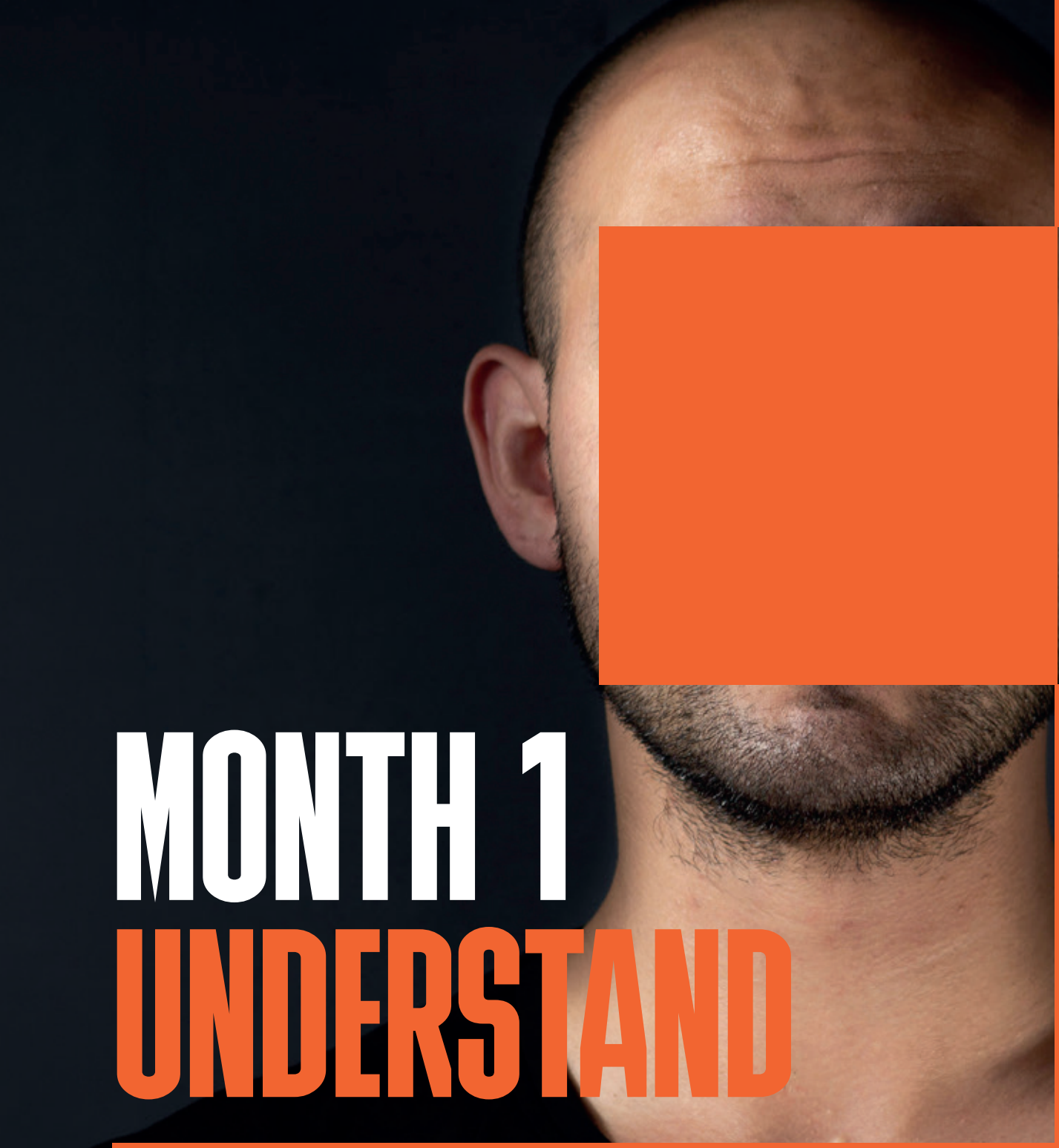
Often, new CISOs walk in and immediately start mapping the network, cataloguing assets, and reviewing security policies. It feels productive and professional, but it's almost entirely beside the point.

So what do the ones who thrive do? They map the P&L before they map the network. They find the Shadow Risk Register – the risks people actually talk about at the coffee machine or at the end of the Zoom call when the other attendees have signed off. They audit the culture, not just the controls. And they speak to their peers, and 'up', in terms of commercial impact, not CVE scores.

This guide reframes those critical, first 90 days around what actually matters: understanding the business, finding ground truth, and making decisions that protect value – and avoid security theater.

At the end of this guide, you'll find a complete **90-Day Action Plan** that breaks down every action, outcome, and timeline. The sections that follow provide the context and reasoning behind those actions. Read the guide for the "why," reference the table for the "what" and "when."

Let's get into it.



MONTH 1
UNDERSTAND

The Core Question

"What does the business actually need from security, and what does it think it needs?"

Your first 30 days aren't about fixing things. They're about understanding what's believed to be working and actually broken versus what people say is broken. These are rarely the same thing.

The instinct is to dive into technology: review the SIEM, check firewall rules, audit access controls. Resist it. If you start there, you'll optimize for the wrong things. You'll speak a language the business doesn't understand and burn through your 'honeymoon period' credibility trying to get budget for problems they don't think they have.

Start with the business. Everything else flows from there.

1.1 - Map the revenue, not the network

When I took on my first CISO role, I spent the first week building an asset inventory. It felt important. How can you protect what you don't know you have? Two weeks in, the CFO asked me a simple question: *"If we lose access to our customer payment system for 48 hours, what happens?"*

I had no idea. I knew we had servers in that environment. I knew we had redundancy. I knew the last pen test found several medium-risk vulnerabilities. But I couldn't tell them what it meant for revenue, customer retention, or regulatory standing. I wasn't speaking their language.

The business cares about revenue, reputation, and whether they can keep operating. Security exists to protect value creation, not infrastructure for its own sake.

The successful CISOs I've worked with start by mapping revenue streams, not networks. They ask:

- *What are the top 3-5 revenue streams in this business?*
- *What processes enable each stream?*
- *If this process stops for 24 hours, 48 hours, a week, what happens?*

Document this gap. You'll address it later.

A note on EU vs US: EU: Revenue often ties directly to GDPR compliance. US: More fragmented (PCI, HIPAA, state privacy laws). Either way, map revenue to regulatory dependencies.

1.2 - Find the Shadow Risk Register

The official Risk Register you've inherited looks great. It's well-formatted. Risks are categorized by likelihood and impact. Mitigations are documented. Everything has an owner.

It's also a lie.

The real risks live in what we call the Shadow Risk Register. It's not written down anywhere. It's what people talk about when certain others aren't in the room, in Slack DMs, or after a few drinks at the company off-site. It's the stuff everyone knows but nobody wants to formally acknowledge or treat.

One of the CISOs in my network put it this way: *"Look for the gaps between policy and practice, where real culture overrides written policy. That's where your exposure lives."*

I worked with a financial services company where the official policy mandated all internal communications go through approved, encrypted channels. But in practice, the executive team expected instant responses on WhatsApp. Nobody documented this. But every sensitive decision, every customer issue, every regulatory discussion? WhatsApp.

That's the Shadow Risk Register.

The distance between Board confidence and engineering reality is what we will call the Delusion Gap. Your job in Month 1 is to measure it.

1.3 - Audit the culture, not just the controls

I watched a company with excellent technical controls get breached because a user (yes, with too many privileges...) was too afraid to report that they'd clicked a phishing link.

Culture isn't about posters on the wall or training videos. It's about what people do when nobody's watching. Whether mistakes get hidden or reported. And who really makes security decisions (often not the security team).

Psychological safety. The hidden control.

> **Ask one question.**
> Do people hide mistakes? If you don't know, the answer is yes!

If your people are afraid to report a clicked link, you have zero visibility into what's actually happening. Your incident response plan is worthless if nobody tells you there's an incident until it's too late. ALL of your people are your business' cyber guardians – they need to know they can speak up without negative ramifications.

THE SHADOW CISOS

In every organization, there are people I call Shadow CISOs.

They're not on the security team. They might be senior developers, IT leads, or infrastructure architects. But they're the ones making real security decisions every day, often by ignoring or working around official policy. Sometimes, unknowingly.

They often do this because the official policy is too slow, bureaucratic, or disconnected from operational reality. Security should speed UP your organisation's rate of innovation and change through the confidence it inspires, not slow it down.

You can fight those that push back against failing security controls, or you can co-opt them. Fighting them is exhausting – especially when they're usually on they're doing so for the right reasons. Co-opting them turns one of your biggest risks into your biggest asset.

1.4 - Understand compliance as "License to Operate"

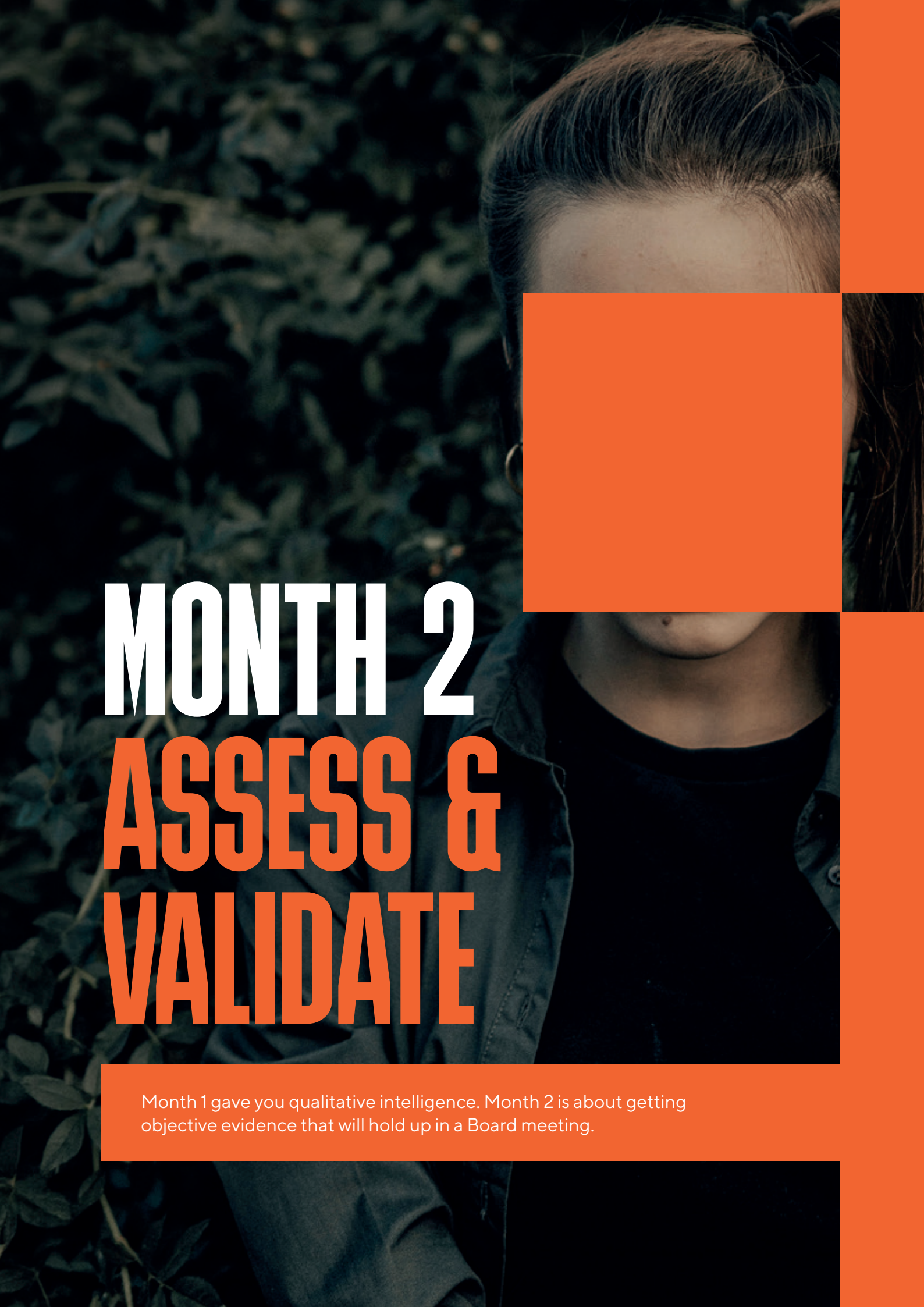
Compliance isn't just about avoiding penalties. **It's your license to operate.**

If you lose PCI status, can you still process payments? If you lose HIPAA compliance, can you still handle patient data? If you breach GDPR badly enough, can you still do business in Europe? For some organizations, the answer is no. That makes compliance existential, not bureaucratic.

In Month 1, understand what you're obligated to protect and ensure leadership understands the stakes. Build the business case, don't fix gaps yet.

By day 30, you should know what the business values, where perception diverges from reality, and who holds the real power.

**See the 90-Day Action Plan for specific timelines and actions.*



MONTH 2
ASSESS & VALIDATE

Month 1 gave you qualitative intelligence. Month 2 is about getting objective evidence that will hold up in a Board meeting.

2.1 - Measure the delusion gap

Traditional assessments (compliance audits, vuln scans) won't help. You need to see your organization the way an attacker sees it, not in some aging report, but right now.

The offensive security approach

Offensive security assessments (red teaming, full-spectrum cyber attacks) see things compliance audits miss entirely.

Companies pass pen tests with minor findings, then get compromised by realistic attack simulations days later. Why? Pen tests have artificial boundaries. Attackers don't. An offensive assessment gives you real exposure data and evidence the Board can't dismiss as opinion.

Why this matters politically

When you're new, delivering bad news is risky. If it's just your opinion ("I think we're exposed here"), you're easy to dismiss. If it's backed by an independent offensive assessment ("A realistic attacker compromised our crown jewels in 72 hours"), it's much harder to ignore. You're not the pessimist. You're the messenger of objective reality.

A note on EU vs US: *EU frameworks like CBEST and STAR-FS are regulator-recognized. The US has no federal equivalent, but the principle is universal: adversarial testing reveals ground truth.*

2.2 - The ransomware test

Let me be blunt: if you can't recover from a ransomware attack without paying, nothing else you do matters. It doesn't matter how good your firewall is; or that you have a perfect patching cadence; or your SIEM has 99.9% uptime. If an attacker encrypts your systems and you can't restore from backups, you're going to pay the ransom or most likely go out of business. Full stop.

"We have backups" ≠ "We can restore from backups"

Every CISO says they have backups. Most of them do. The question isn't whether backups exist. Can you restore from them under realistic conditions? RPO? RTO? You get the point.

'Realistic conditions' means:

- Your primary systems are encrypted;
- Your backup admin's credentials might be compromised;
- Your Active Directory might be gone;
- You're under time pressure (customers are angry, the Board is panicking, media is calling);
- Some of your backups might be corrupted or also encrypted;
- Working late is not an option for at least 30% of your key staff (hey, life also gets in their way).

Most organizations have never tested it. And when they do, they find out the answer is 'no'.

EU vs US considerations: *EU: NIS2 and DORA mandate resilience testing. US: sector-specific requirements (SEC disclosure rules, state regs). Resilience is becoming table stakes everywhere.*

2.3 - Validate your people (the human layer)

In Month 1, you audited the culture. Now you need to validate whether that culture holds up under realistic pressure.

The new starter problem

New starters are one of the highest-value targets for attackers, and most organizations completely ignore this.

Think about it from an attacker's perspective. New employees are:

- Eager to help and prove themselves;
- Less familiar with internal processes;
- Less likely to question unusual requests;
- Often given broad access quickly (especially in IT or support roles).

Attackers scrape LinkedIn for new hires, especially in IT support or helpdesk roles. Then they call or email, impersonate a senior executive, and ask for something urgent. *"I'm locked out of my account and I have a board meeting in 10 minutes. Can you reset my password?"* The new starter wants to be helpful. They don't want to seem obstructive or slow. So, they do it. And just like that, the attacker has access. That's often one of the ways CovertSwarm's ethical hackers break in to our clients...

Most organizations address this in week three or four. By then, the damage is done.

Social Engineering: The Universal Bypass.

Phishing is the obvious example, but it's not the only one. Vishing (voice phishing), physical tailgating and pretexting all work. Humans are trusting, busy, and conflict-averse. You need to know how vulnerable your people are. Not hypothetically. Actually.

> **By day 60, you have objective data on your exposure.**
> Month 3 is about deciding what to fix first and getting buy-in.

MONTH 3
DECIDE

The Core Question *"What do I fix first, and how do I get buy-in?"*

You have data. Now decide what to fix first and get buy-in. This is where most new CISOs stumble.

3.1 - Prioritize for commercial impact, not CVE scores

Here's a truth that took me too long to learn: the Board doesn't care about vulnerabilities. They care about business continuity, reputation, and shareholder value. You can walk into a Board meeting with a list of 500 medium-severity vulnerabilities and watch their eyes glaze over. Or you can walk in with three critical business risks articulated in terms they understand, and you'll have their full attention.

CISOs who thrive translate cyber risks into commercial impacts: revenue loss, regulatory penalties, customer churn, reputational damage. The ones who struggle talk CVE scores, and lose their audience.

How to Prioritize When You Can't Fix Everything.

You have limited budget, headcount and political capital. If you try to fix everything, you'll fix nothing and burn out your team in the process.

Here's the framework

1. Map findings to revenue streams.

For each finding, ask: *"If exploited, which revenue stream is impacted?"* Example: *"Customer database compromise = $12M revenue loss from 15-20% churn, plus GDPR fines up to 4% of revenue."*

2. Identify "license to operate" risks.

Which findings directly threaten your ability to maintain compliance or regulatory standing? If exploited, do you lose PCI status? HIPAA compliance? The ability to operate in the EU?

These aren't just *"compliance issues."* They're existential

3. Focus on operational resilience.

Which findings directly impact your ability to survive and recover from an attack? Can't restore from backups? That's priority one. Weak identity and access management that would let an attacker move laterally across your entire environment? Priority two.

Prevention is great. Survivability is essential.

4. Consider exploit likelihood and attacker motivation.

Not all vulnerabilities are equally likely to be exploited. A critical vulnerability in an internet-facing system that processes payments is a much higher priority than the same severity vulnerability in an internal HR system that requires significant access to reach.

Think like an attacker. What would they target first? Start there.

3.2 - Deliver the hard news (and make it land)

You found bad news. Validate it. And again. Now deliver it without panic, blame, or the risk of losing credibility.

The framing problem

When you're new, bad news gets dismissed: *"The last CISO said we were fine. Are you sure you're not being overly cautious?"* This is why objective evidence matters. Opinion is easy to question. Independent offensive testing isn't.

One CISO I worked with put it well: bringing in an external offensive assessment in your first 90 days lets you deliver fresh, unbiased findings that show what a real attacker sees today. It's not *"new starter pessimism."* It's *"here's what an adversary would do, demonstrated by people who think like adversaries."*

Delivery framework

Here's how to structure the conversation

1. Acknowledge the current state without assigning blame.

"The security program has served the business well to this point. As the business has scaled and the threat landscape has evolved, we have gaps that need to be addressed."

Don't throw your predecessor under the bus. You're not here to point fingers. You're here to solve problems.

2. Present findings in business impact terms.

Not: *"We have 47 critical vulnerabilities and inadequate segmentation."*

Instead: *"Our assessment revealed that an attacker could gain access to customer payment data and potentially disrupt transaction processing within 48-72 hours. This would result in estimated revenue loss of $3-5M, mandatory breach notification affecting 2M customers, and potential regulatory penalties under GDPR and PCI."*

3. Provide context and comparison.

How does your security posture compare to peers? Are the findings surprising, or consistent with what you'd expect for an organization of your size and maturity?

Context prevents panic. *"These findings are significant, but they're not unusual for a company at our stage. What matters is that we address them systematically."*

4. Present the plan with clear milestones.

The Board doesn't just want to hear problems. They want to know you have a path forward.

Here's what we're going to do [be specific]:

- Next 30 days: Address the three highest-impact risks
- Next 60-90 days: Implement foundational resilience capabilities
- Next 6-12 months: Build out the broader security program [high level]

5. Be clear about trade-offs and resource requirements.

If you need budget, headcount, or organizational changes, say so. And be clear about the trade-offs.

"We can address Tier 1 risks with current resources, but it will require delaying two other IT projects. Alternatively, we can bring in contract help for $X, which lets us move faster without disrupting other work."

3.3 - Build your first 12-month roadmap

The 90-day mark is your credibility checkpoint. The Board is evaluating whether you're strategic or just firefighting. A roadmap shows you're thinking long-term, not just reacting to the crisis of the day.

Your roadmap doesn't need to be perfect. It will change as you learn more. But it needs to exist, and it needs to be grounded in the business priorities you've identified.

Here's a framework that works.

The roadmap structure

Months 4-6: Operational resilience foundations

- Fix backup/recovery gaps, improve incident response, address Tier 1 risks, establish baseline monitoring.

This phase is about making sure you can survive the next major incident. Everything else is secondary.

Months 7-9: Continuous security validation

- Establish continuous offensive testing, regular social engineering assessments, threat intelligence capability, and address Tier 2 risks.

This phase is about creating feedback loops, so you know when things break before an attacker exploits them.

Months 10-12: Culture, capability, and maturity

- Integrate security into onboarding, co-opt Shadow CISOs, improve awareness programs, mature key processes, and address Tier 3 risks.

This phase is about sustainability. You're building a program that works without you being the bottleneck.

By day 90, the Board should see you as someone who understands the business, knows the real exposure, has a credible plan, and speaks their language. That's success.

**See the 90-Day Action Plan for communication and roadmap-building actions.*

A final thought

The first 90 days aren't about perfection

I've been 'that' CISO. I've seen the pressure, the complexity, the impossible trade-offs. I've also spent years on the offensive side, seeing organizations through a pure, attacker's eyes.

Let's be honest: you're not going to fix your security program in 90 days. If anyone tells you otherwise, they're selling something...and it's probably snake oil. What you can do is understand the business, find ground truth, and make strategic decisions about what matters most.

The organizations that survive aren't the ones with perfect security programs. They're the ones with CISOs who understand the business, speak clearly about risk, and make hard decisions when it counts. Your first 90 days set the tone for everything that follows. Understand before you act. Test before you trust. Speak truth backed by evidence.

The Board doesn't need you to be perfect. They need you to be credible, strategic, and focused on what actually matters.

MONTH 1: UNDERSTAND

Phase	Action	What you'll achieve	Timeline
Business Alignment	Identify top 3-5 revenue streams and map critical processes supporting each	Know what actually needs protection and speak to Board in business terms	Week 1-2
	Ask the "failure question" for each revenue stream: "If this stops for X hours, what happens?"	Understand concrete business impact of security failures	Week 1-2
	Compare security spend/focus to revenue protection priorities	Identify gap between what makes money and what you protect most	Week 1-2
Reality Check	Talk to people who run things: sysadmins, DevOps, IT support, DBAs (not just security team)	Find the Shadow Risk Register and "unwriteable" risks	Week 2-3
	Document policy vs. practice gaps (approved tools nobody uses, bypassed controls, Shadow IT)	Measure the Delusion Gap between Board perception and ground truth	Week 2-3
	Compare official Risk Register to what engineers actually worry about	Quantify what's missing from official risk documentation	Week 2-3
Culture Audit	Assess psychological safety: "When someone makes a mistake, what happens?"	Know if your incident response will actually work when people are afraid	Week 2-4
	Map the Shadow CISOs (who really makes security decisions by ignoring/working around policy)	Identify key stakeholders to co-opt, not fight	Week 2-4
	Meet with senior stakeholders individually about their security concerns and perceptions	Understand what the organization values and where political landmines are	Week 2-4
	Audit new starter onboarding: when and how is security culture integrated?	Close critical social engineering vulnerability window	Week 3-4
Compliance Strategy	Map compliance requirements to business continuity: "If we lose this, what stops working?"	Reframe compliance as "license to operate," not checkbox exercise	Week 3-4
	Understand EU vs. US enforcement landscape and align with stakeholder concerns	Connect regulatory requirements to business goals leadership cares about	Week 3-4

MONTH 2: ASSESS & VALIDATE

Phase	Action	What you'll achieve	Timeline
Measure Delusion Gap	Commission realistic offensive assessment (red team, not scoped pen test) across digital, physical, social vectors	See your organization the way an attacker sees it with objective evidence	Week 5-7
	Focus assessors on attack chains, not individual vulnerabilities	Understand how weaknesses combine into critical exposures	Week 5-7
	Translate all findings to business impact terms (revenue loss, customer impact, regulatory exposure)	Build evidence-based case for remediation that Board understands	Week 5-7
	Compare findings to official Risk Register	Quantify the Delusion Gap with hard data	Week 5-7
Ransomware Resilience Test	Actually test backup restoration in non-prod environment (not tabletop, actual restoration)	Know if you can survive ransomware without paying ransom	Week 6-8
	Measure RTO/RPO for critical systems and compare to business requirements from Month 1	Identify gaps between what you can do vs. what business requires	Week 6-8
	Simulate degraded conditions: backup admin unavailable, partial storage compromise, 50+ systems simultaneously	Test resilience under realistic pressure, not ideal conditions	Week 6-8
	Document gaps, costs to fix, and risk of not fixing	Build business case for resilience investment	Week 6-8
Validate Human Layer	Run realistic social engineering tests: contextual phishing, vishing against IT support, physical access attempts	Validate culture and identify high-risk groups	Week 6-8
	Focus on high-risk groups: new starters, IT/helpdesk, finance teams, executive assistants	Test groups most likely to be targeted by real attackers	Week 6-8
	Measure reporting rate, not just click/success rate	Assess psychological safety and incident response readiness	Week 6-8
	Specifically audit security integration in new starter onboarding process	Close highest-probability social engineering attack vector	Week 6-8

MONTH 3: DECIDE

Phase	Action	What you'll achieve	Timeline
Prioritize Strategically	Map Month 2 findings to revenue streams and create 3-tier remediation plan (Tier 1: 30-60 days, Tier 2: 60-120 days, Tier 3: 6-12 months)	Know what to fix first based on business impact, not technical severity	Week 9-10
	Quantify each tier in business terms: revenue impact, regulatory exposure, operational downtime	Build resource request backed by financial data Board understands	Week 9-10
	Identify quick wins that demonstrate visible progress in 30 days	Build momentum and credibility while addressing longer-term issues	Week 9-10
Communicate Effectively	Prepare Board presentation focused on business impact, not technical findings (10-15 min max)	Get buy-in for remediation plan and resource allocation	Week 10-11
	Socialize findings with CEO/CFO individually before Board meeting	Ensure executive alignment and avoid surprises	Week 10-11
	Frame findings: acknowledge current state (no blame) + quantify risk in business terms + present plan with milestones + show quick wins	Deliver hard news effectively without panic, blame, or loss of credibility	Week 10-11
	Bring objective evidence (offensive assessment results, test data), not opinions	Establish credibility as truth-teller backed by data	Week 10-11
Build Roadmap	Document 12-month roadmap: Months 4-6 (Resilience), 7-9 (Continuous Testing), 10-12 (Culture/Maturity)	Show strategic thinking beyond firefighting	Week 11-12
	Tie each phase to business outcomes with clear success metrics	Establish accountability and measurable progress	Week 11-12
	Align every initiative to: revenue protection, license to operate, or operational resilience	Ensure roadmap stays business-focused, not security-theater-focused	Week 11-12
90-DAY OUTCOME	**By day 90, the Board sees you as credible, strategic, and focused on business outcomes. You have mandate, resources, and political capital to build a real security program.**		

CovertSwarm®

CREST PEN TEST STAR Intelligence-led PT STAR-FS Intelligence-led PT CBEST

www.covertswarm.com