COURSE · SECURITY BY DESIGN · WEEKS 2–3

You can't secure what you're never told about. *So become the checkpoint they reach first.*

The first skill of Security by Design: turning yourself from "the security guy" into the advisor every project consults before it buys, builds or connects anything, the checkpoint the business cannot route around.

Drawn from real enterprises. This case is composited from shadow-IT discoveries lived through inside real companies. Figures and details are changed for teaching; the pattern is not.

Learning phase · Becoming the security checkpoint **Case** · First CISO of a remote e-commerce start-up

Focus · Get informed early, before the decision is made

WHAT THIS PHASE BUILDS

The skill that makes security impossible to route around.

Everything here trains one habit: being in the room before the decision, not after the breach. Work the case, then rehearse the moves against your own organisation.

- Get informed early about IT needs, before anything is bought or connected.
- Evaluate the risk of a proposed solution fast, so you enable instead of block.
- Propose security measures that actually get accepted.
- Get formal, signed risk acceptance from the business owner.
- Keep the documentation that protects you the day something breaks.

01 THE SITUATION

First CISO, and nobody has called you

You are the first CISO of a fully-remote e-commerce start-up. For three months the business has moved fast, buying tools, wiring up integrations, standing up servers, and none of it has crossed your desk. Then you start looking.

Your role

The company's first-ever CISO. No predecessor, no process, no precedent to point to.

The company

A fully-remote e-commerce start-up. Speed is the culture; tooling gets bought on a card.

The data

300,000 prospect and customer records, the crown jewels, already spread across systems you've never seen.

Your status

Nobody has consulted you once. Decisions get made and you find out later, if at all.

02 WHAT YOU DISCOVER

Five things done without you

Three months of shadow IT, each one a decision the business made alone. For each, the real exposure it created.

1 **A SaaS CRM from an unknown vendor**

Marketing bought a SaaS CRM from a company nobody has heard of, and moved all 300,000 prospect and customer records into it.

Risk: 300k PII records now live with an unvetted third party, with no security review and no data-processing agreement, a direct GDPR exposure.

2 **A cloud service wired into the mail servers**

The accounts-receivable team connected a cloud solution to the company mail servers to receive invoices.

Risk: a third party now sits in the mail flow, a ready-made path for invoice fraud, business-email compromise and quiet data exfiltration.

3 **A site-to-site VPN to an outsourcer**

A site-to-site VPN links an IT outsourcer (ESN) straight into your Azure data centre, because they run your SAP server.

Risk: a standing tunnel from someone else's network into yours. Their breach becomes your breach, and nobody has mapped what it can reach.

4 **Nameless, non-expiring AD accounts**

Accounts exist in Active Directory set to "password never expires", with no owner name, and nobody knows what they are for.

Risk: classic orphaned or backdoor accounts, persistent credentials no one can attest to, and a gift to any attacker.

5 **Azure servers with SSH open to the internet**

Several servers in your Azure subscription have SSH exposed to the internet. Their purpose is unknown, but they are logging activity.

Risk: internet-facing attack surface that can be scanned and brute-forced, and may already be compromised.

03 WHY IT HAPPENED

None of this is sabotage

Every one of these was a reasonable person trying to get their job done. Shadow IT is not malice, it is the predictable result of a security function nobody was required, or able, to consult. Fix the pattern, not the people.

01 **No way in**
There is no known, easy path to run something past security, so busy teams simply don't.

02 **Security reads as a blocker**
If the expected answer is "no", or "in three weeks", people route around the gate to keep moving.

03 **No visibility**
You can't see decisions as they happen.

THE QUESTION

What do you do to stay informed of all of this, and become the security checkpoint the company can't do without?

04 THE PLAYBOOK WORKSHOP

How you become the checkpoint

We build these five moves together in the workshop. For each, you work out how it applies to your own organisation and leave with your own version written down.

1 Get informed early
Where in your organisation are IT decisions actually made, and how do you earn a seat before anything goes live?

2 Triage risk fast
What does a proportionate, same-day review look like for you, so security enables rather than blocks?

3 Propose measures that land
How do you frame a control in the business owner's language so it actually gets adopted?

4 Get signed risk acceptance
What is your one-page risk-acceptance format, and who has to sign it?

5 Document everything
What do you keep, and where, so the record protects you the day something breaks?

05 FIRST 90 DAYS WORKSHOP

What to do with what you found

Take the five discoveries from the case. For each, decide together how you would contain it now, and the process that would stop the next one happening in the dark.

FINDING	CONTAIN IT NOW	PROCESS THAT PREVENTS A REPEAT
Unknown SaaS CRM		
Cloud service on the mail flow		
ESN site-to-site VPN		
Nameless non-expiring accounts		
Public SSH servers		

WHAT THIS CASE TEACHES

Four habits of a checkpoint no one bypasses

Whatever the company, being consulted early comes down to the same few habits. They work in any organisation.

01 Be a partner, not a gate
The business routes around blockers and consults advisors. Make being helpful your security strategy.

02 Get visibility at the source
You can't be consulted on what you can't see.

03 Make the secure path the fast path
A same-day "yes, and here's how" beats a three-week "no" every time, and keeps teams coming to you.

04 Put the risk in writing, signed
Formal risk acceptance turns your "no" into the owner's decision, and is the documentation that saves your career the day something breaks.