FOUNDER FIRE CODES™ · ADVANCED FIRE

09

THE NO-BACKUP-PLAN BREAKDOWN

If you were unreachable for a week, things wouldn't just slow down. Some of them physically could not happen.

DEPENDENCY TYPE SYSTEMS & INFRASTRUCTURE

HOW IT SOUNDS "IF I VANISHED FOR A WEEK, THINGS COULDN'T RUN."

TIME TO FIRST RELIEF ONE AFTERNOON — THE ACCESS MAP ON PAPER

FIRE DANGER — HOW FAST THIS ONE COMPOUNDS

SLOW BURN STEADY FAST **FIVE ALARM**

9.1 THE SCENE

Run the drill in your head. It's Tuesday morning, and you are unreachable for seven days. Not a beach-with-wifi unreachable — actually gone. Phone dead, laptop closed, nobody can raise you. What stops?

Walk it honestly. Payroll runs Friday — who approves it? The approval pings *your* phone. The ads account lives under your personal email; if the card on file fails, the campaigns stop and the recovery code goes to a phone nobody else can get into. Your ops lead needs to add a contractor to the project tool — you're the only admin. The client portal is due for its renewal this month, on your personal card, and the receipt will land in an inbox no one else can open. Two-factor codes for the bank, the payment processor, the email platform: your phone, your phone, your phone.

By Thursday of your imaginary week, your very capable team — people who could absolutely do the work — are locked out of doing it. Not because they lack skill or judgment. Because the company's physical wiring runs through your pocket. Every tool got set up in a hurry, by you, with whatever email and card was handy, and "handy" was always yours.

Founders file this under "someday" because it costs nothing on a normal day. That's the trick of it. This is the only fire on the list that produces zero smoke until the exact moment it produces nothing but — a family emergency, a hospital stay, or honestly just the first real vacation you've earned — and by then it has stopped being a fire at all. It's a wall.

YOU KNOW THIS FIRE IS BURNING WHEN

- Critical logins live in your head, your phone's notes app, or your personal password manager.
- Core tools are registered to your personal email and billed to your personal card.
- You're the only admin on at least three systems your business can't run without.
- Two-factor codes for the bank, payroll, or payment processor go to your phone alone.
- The team pings you for access — a shared doc, a tool seat, a permission — at least weekly.
- Renewals surprise you: subscriptions charge, domains near expiry, and no list of any of it exists.
- Nobody, including you, could produce a complete list of the tools the business runs on.
- Your honest answer to "what happens if you're unreachable for a week?" is a nervous laugh.

9.2 WHAT'S ACTUALLY BURNING

This is Systems & Infrastructure Dependency: the company's tools, access, and permissions are wired to you as a person instead of to roles in a company. It's the most literal dependency in the whole taxonomy. The others live in your head — knowledge, judgment, standards. This one lives in your accounts. Fires 01 through 08 make you the mental single point of failure; this one makes you the *physical* single point of failure, and physics doesn't negotiate.

6-10
RED ROWS ON A TYPICAL FIRST ACCESS MAP

2 HRS
TO BUILD THE MAP — ONE HONEST AFTERNOON

1
PAGE OF CONTINUITY PLAN. NOT A BINDER

How did it get this way? Innocently, every time. The business was born inside your personal accounts — your email signed up for everything, your card ran the subscriptions, your phone caught the codes — because in year one, you *were* the company and there was nothing else to wire anything to. Then the company grew, and nobody ever went back and rewired. Every new tool followed the path of least resistance, which was always you. There was no decision to centralize everything through the founder. There was just never a decision not to.

The common fix is sharing a few passwords when someone gets blocked — a login pasted into Slack, a 2FA code read out over a call, "just use my account for now." That isn't a fix; it's a leak with your name on it. Now credentials float around messages, nobody knows who has what, security is worse than before, and the structure is unchanged — everything still routes to you; there's just a trail of exceptions behind it. The real fix isn't sharing your access. It's ending the era of *your* access — moving from person-based wiring to role-based architecture, where the company owns its accounts and people hold access because of the seat they sit in.

> **FIRE WATCH**
>
> Some founders keep this wiring on purpose, quietly, because holding the keys feels like holding the company — if everything runs through your accounts, nobody can ever really push you out, lose your stuff, or surprise you. Name that fear if it's yours, and then notice what it's actually costing: you've made yourself the thing that can never rest. Control that requires your constant availability isn't control. It's a shift you can never clock out of.

> **Your company doesn't have an infrastructure problem. It has your phone number.**
>
> FOUNDER FIRE CODES™

9.3 THE RESPONSE PLAN

The response runs from map to drill: see the wiring, fix the dangerous rows, move ownership to the company, name the backups, write the plan, then test it for real. First relief comes the same afternoon you build the map — dread you can see is instantly smaller than dread you can't.

1. BUILD THE ACCESS MAP
2. KILL THE RED ROWS
3. MOVE OWNERSHIP OVER
4. NAME THE BACKUPS
5. WRITE THE CONTINUITY PAGE
6. RUN THE VANISH DRILL

1 BUILD THE ACCESS MAP — ONE AFTERNOON, NO EXCUSES

One spreadsheet, every tool the business touches. Walk your card statements and your inbox's "welcome to" emails to find the ones you've forgotten. For each: what it does, whose email owns it, who else can get in, what card bills it, where the 2FA goes, and what breaks if it locks. Two hours, maybe three with coffee. This map is the entire diagnostic for this fire — and steps 2 through 6 are just working its rows.

TOOL	ACCOUNT OWNER	OTHER ACCESS	BILLING	2FA	IF IT LOCKED TOMORROW
Payment processor	Founder personal email	None	Company card	Founder phone	No payouts, no refunds — revenue frozen
Email platform	Founder personal email	1 seat (marketing VA)	Founder personal card	Founder phone	No campaigns, no automations, list unreachable
Project management tool	Company email	Whole team; founder sole admin	Company card	Founder phone	Work continues; nobody can add or change anything

Then score each row simply: red means single-owner and business-critical, amber means critical with partial coverage, green means covered. Most founders find six to ten reds on the first pass. That number is your dread, quantified — and now it's a work queue instead of a feeling.

Build the map with your ops lead beside you if you can. They'll remember tools you forgot, they'll learn the terrain they're about to help hold, and the exercise itself starts transferring the network diagram out of your head — which, you'll notice, is this whole book's favorite move.

2 KILL THE RED ROWS FIRST

Triage by what stops the business coldest: money movement first (payment processor, bank, payroll), client-facing systems second (delivery tools, client portal, scheduling), everything else after. For each red row this week: add a second admin, move the 2FA to a method a backup can reach — an authenticator app on a shared vault, not your personal cell number — and confirm the recovery email isn't another account only you can open. Recovery paths are where this work quietly fails: a second admin whose reset email routes to your inbox is a backup in costume.

3 MOVE OWNERSHIP TO THE COMPANY

Rewire the accounts themselves: primary registration to company-owned email addresses (role addresses like ops@ beat personal ones — people leave; roles don't), billing to company cards, credentials into a proper shared password manager with role-based vaults — ops sees ops tools, marketing sees marketing tools, and the emergency vault stays sealed for step 5. Nobody pastes a password into a chat again, including you. This step is tedious and wildly unglamorous, which is why it never got done. Batch it: three accounts a week, reds first, and the whole migration is done inside two months.

Expect a little grief in the middle of it — some platforms make ownership transfers genuinely annoying, and one or two will require support tickets and patience. Do those anyway, and do them now, on a calm week, with you available to approve the transfer. The platforms that make ownership hardest to move are precisely the ones that would be hardest to recover in an emergency, which makes them the most important rows on the map, not the skippable ones.

4 NAME A BACKUP OWNER FOR EVERY CRITICAL SYSTEM

Access by role, and a named human backup per critical system — someone who can administer it, not just log in. The distinction matters: a backup who can view the payment processor but can't issue a refund or re-run a failed payout is scenery. Put the names on the access map, then close the loop the way Chapter 1 of the Installation Guide taught: tell them, walk them through the system for an hour, and put a fifteen-minute refresher on the calendar quarterly. An untested backup decays into a name in a spreadsheet within six months.

5 WRITE THE CONTINUITY PLAN

One page, boring on purpose, answering exactly one question: the founder is unreachable for seven days — who does what? Resist the urge to write the forty-page disaster binder; nobody opens a binder mid-emergency. One page gets read. Who runs payroll, who holds client communication, who can spend money and to what limit, who opens the sealed emergency vault and under what conditions, and who decides anything the page doesn't cover (your ops lead, probably — name them). Store it where the team can find it without you, which is the entire point. Yes, it feels morbid to write. Write it anyway; it's an hour, and it converts your worst-case scenario from a company crisis into a bad week.

6 RUN THE VANISH DRILL

Maps and plans are theory until tested, so test: pick a half day, announce it as a drill, and go dark. The team runs everything through the new wiring — vaults, backups, continuity page — and logs every single block: every password that wasn't in the vault, every permission that fell short, every "we'd normally just ask her" moment. Every block is a gap found on a calm Tuesday instead of a terrible one, which makes the drill's block list the cheapest consulting your infrastructure will ever get.

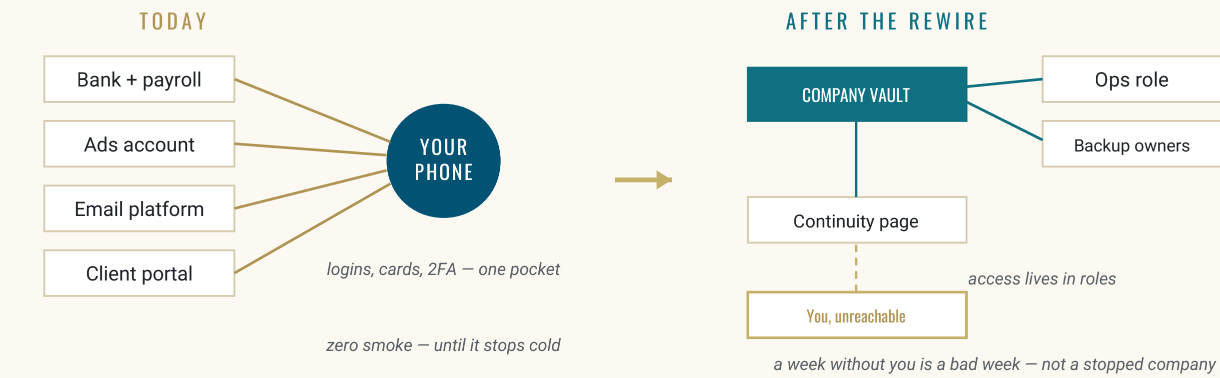
> **SAY THIS WHEN YOU ANNOUNCE THE DRILL**
>
> *"Next Thursday morning, I'm going dark from nine to one — on purpose. Pretend you can't reach me, because that's the drill: everything runs on the vault, the backups, and the continuity page. This isn't a test of y'all — it's a test of the wiring, and honestly I expect us to find holes. Every time you hit a wall, don't work around it quietly — write it down. The wall list is the whole prize. Friday we'll fix what it found, and next quarter we'll do it again for a full day."*

Debrief the drill within a day, while the blocks are fresh, and sort the list into three buckets: missing access (vault and permission fixes — usually same-week work), missing knowledge (the answer existed only in your head — those become documentation), and missing authority (the person could act but didn't feel allowed to — those route back to the decision boundaries in the Installation Guide, Chapter 2). That third bucket surprises founders every time. Half of "we couldn't reach you" turns out to mean "we didn't know we were allowed," which is a cheaper fix than any software — and a reminder that this fire's wiring runs through permission as much as passwords.

9.4 THE PREVENTION PLAN

The rewiring is done. Prevention means it stays done — because infrastructure drifts back toward the founder one convenient shortcut at a time, and every new tool is a fresh chance to rebuild the old wiring.

THE REWIRE — FROM YOUR POCKET TO THE COMPANY'S ARCHITECTURE



Person-based wiring fails all at once, and only on the worst day. Role-based architecture — vault, backups, continuity page — keeps running when your phone doesn't.

WIRE THE ON-RAMP AND THE OFF-RAMP

New tools follow a standing rule from day one: registered to a company role address, billed to a company card, credentials in the vault before first use, an owner and backup named at signup. Make it a five-line checklist inside whoever-buys-software's workflow — the rule only holds if it's easier to follow than to skip. And yes, the rule applies to you hardest of all, because you're the one most likely to sign up for something on a Saturday with whatever email autofills. Departures get the mirror image: an offboarding checklist that revokes access the same day, rotates anything they touched, and reassigns their system ownerships by name. A company that only ever adds access is one resignation from a security problem and two from an archaeology project.

DON'T FORGET THE OUTSIDE WIRING

Some of your infrastructure lives outside your login screens, and it's wired to you just as tightly. Your bookkeeper, your accountant, your attorney, your bank contact — do any of them know anyone at your company besides you? If every professional relationship the business depends on routes through your cell phone, those are red rows too; they're just not on a card statement.

Introduce your ops lead to each of them this quarter — a fifteen-minute call apiece — and make sure the bank has a second authorized contact who can actually get questions answered. Same treatment for the paper layer: the operating agreement, insurance policies, key contracts, and where they physically live. The continuity plan should say where the documents are, not just who does the tasks.

REVIEW ACCESS QUARTERLY

CHECK	CADENCE	OWNER	LOOKING FOR
Access map refresh	Quarterly	Ops lead	New tools off-map, red rows creeping back, stale seats
Backup touch	Quarterly	Each backup owner	Fifteen minutes inside their system — can they still do, not just see
Renewal calendar review	Quarterly	Ops lead	Upcoming renewals, domains, certificates — zero surprise charges
Vanish drill	Twice a year	Founder schedules; team runs	A shrinking block list — the trend is the metric

Notice the owner column: it's the ops lead, not you. Infrastructure guardianship is itself a system that shouldn't route through the founder. Your only recurring job on this list is scheduling your own absence — fitting, honestly. And when the quarterly review finds nothing wrong three quarters running, don't cancel it; shorten it. The review existing is why there's nothing to find.

DOCUMENT THE WIRING ITSELF

The last layer is a simple systems doc: what tools exist, what each is for, how they connect — what feeds what, which automations matter, where the bodies are buried. Not for you; you know it. For the version of your company where you're not the walking network diagram, and for every future hire who'd otherwise reconstruct it by asking you one question at a time. An afternoon to write, an hour a quarter to keep true — and it pairs with the continuity plan as the two documents that make your company survivable, not just successful.

★ FIRE MARSHAL'S NOTE

Keep one printed copy of the continuity plan — on paper, in a place two people know about. The lockout scenario you're planning for can include the wiki, the vault, or the whole workspace being the thing nobody can open. Paper is the only system on the map with no login, no renewal, and no 2FA.

9.5 MAKE IT YOURS

YOUR RED ROWS

The three systems that scare me most on the access map: ____________________, ____________________, ____________________

YOUR VAULT

The password manager we're standardizing on, and the date every credential is in it: ____________________

YOUR BACKUPS

Backup owner for money systems: ____________________ · client systems: ____________________ · marketing systems: ____________________

YOUR CONTINUITY PAGE

Who decides in my absence: ____________________ — and where the one-page plan lives: ____________________

YOUR DRILL

Date of the first vanish drill: ____________________ — and who owns the block list afterward: ____________________

9.6 PROOF IT'S OUT

- [ ] The access map exists, is current within the quarter, and has zero red rows.
- [ ] Every business-critical system has a tested backup owner who can administer it, not just open it.
- [ ] No core account lives on your personal email, card, or solo 2FA anymore.
- [ ] A vanish drill ran, produced its block list, and the fixes shipped inside a week.
- [ ] The team resolved an access problem — a lockout, a permission, a renewal — and you learned about it afterward.
- [ ] You took genuinely unreachable time off, and the infrastructure didn't send a single flare.

Relight warnings: a new tool shows up registered to somebody's personal email — including yours, especially yours, because the signup was faster that way. A password lands in a chat thread "just this once." The quarterly review slips twice. Or you notice access requests pinging your phone again, which means the wiring found its way home. None of these is a crisis on the day it happens. All of them are the first thread of the old web. Pull them out the week you see them.

> **Build a business that misses you when you're gone. Not one that stops.**
>
> FOUNDER FIRE CODES™

LUXE BUSINESS BACKEND™ · FOUNDER FIRE CODES™