

NOBODY OWNS YOUR TECHNOLOGY

All of it. One owner.

The 90-Day Reset for professional services firms.



PETER NELSON

IT • Cyber • Phones • Internet • Website • Search • Ads • AI

Nobody Owns Your Technology

All of it. IT, cyber, phones, internet, website, search, ads,
AI. One owner. The 90-Day Reset for professional ser-
vices firms.

PETER NELSON, DIRECTOR, CX IT SERVICES

Contents

Introduction: Who owns your domain name?	5
PART ONE: WHAT YOU'VE GOT	8
1. Technology is the backbone	9
2. The pointing problem	15
3. IT support. Tickets, not outcomes	23
4. Cyber. The baseline nobody set	27
5. Phones and internet. The cable in the wall	37
6. Websites. The brochure	40
7. Digital marketing. The leak	44
PART TWO: WHY IT'S BROKEN, AND WHAT FIXES IT	51
8. Why this isn't working anymore	52
9. How CX365 brings it all together	56
10. The four pillars, and the order they go in	62
PART THREE: THREE WAYS TO FIX IT	67
11. Three ways to fix it	68
12. Do it yourself. The way you're probably doing it now	69
13. Done with you. Own Your Technology	72
14. Done for you. The best way	76
15. The first 90 days	83
16. Growth. How it scales with you	91
Questions partners ask	96
One last thing	100

THE PROMISE

By the end of this book you'll know why your technology costs what it costs and does less than it should. You'll know what a firm your size should have, in every one of the eight things on the cover. And you'll know the three ways to fix it, including the one where you don't have to.

No 40-page proposal. No sales call. No three-year contract you signed because you were tired.

WHO THIS IS FOR

You run, or help run, a law firm, an accounting practice, a medical practice or a financial services business somewhere in Australia or New Zealand. Ten staff, or a hundred. You've got an IT provider. You've probably got a marketing agency, or had one. You've paid for marketing that sort of worked. Somebody set up some automation once.

Nobody owns the whole thing.

You're not reading this because your technology is a disaster. It's probably fine. Fine enough that nobody's fixed it.

That's who this is for.

WHO THIS IS NOT FOR

Firms shopping for the cheapest quote. Good luck, sincerely.

Firms that want the lights kept on and nothing else. There are plenty of people who'll do that.

HOW THIS BOOK IS LAID OUT

Part one is what you've got. Eight short chapters, one for each thing you're paying for, and what's probably wrong with it. Read the ones that sting.

Part two is why it's broken, and the one idea that fixes it.

Part three is the three ways to fix it. Yourself, with us, or by us. Then what the first 90 days look like, and what happens as you grow.

Read it in order if you can. The order is the argument.

Introduction: Who owns your domain name?

Nearly eight years ago I quit a full-time job to start an IT company with a strange name.

CX IT Services. The CX stands for customer experience.

Not “Nelson IT”. Not “Melbourne Managed Services”. Not something with “Tech” or “Cloud” in it. I’d spent the best part of two decades inside the IT industry by then, and I’d seen what it sold. It sold tickets. Response times. Hours. It sold keeping the lights on, and it was very good at telling you how many lights it had kept on.

What it never sold was the experience of being a client.

I’d played footy most of my life, and anyone who has will know the phrase “one percenters”. The smother. The shepherd. The chase-down tackle nobody puts in the highlights. The little things that don’t show up on the stat sheet and win you the game anyway.

That’s what I wanted to build. An IT company made of one percenters.

So that’s where the name came from. This book is about what I learned after.

THE QUESTION

Over 26 years I've been inside a lot of professional services firms. Law. Accounting. Medical. Financial planning. More than a hundred of them now across Australia and New Zealand.

And there's one scene I've watched play out so many times I could write the script.

A partner sits down with me. Decent firm. Thirty people, say. They've got an IT provider. They've got a marketing agency, or they had one until the retainer started to feel like a donation. Someone set up a CRM once. Someone else built an automation that emails new clients, and nobody's sure if it still runs.

I ask one question.

"Who owns your domain name?"

And they pause.

Not because they're not smart. These are some of the sharpest people I know. They pause because the honest answer is "the web guy, I think, or maybe IT, or it might be in the old practice manager's name". And the domain name is the front door to everything. Email. Website. The logins for half their software.

Three vendors. Each good at their bit. None of them responsible for the whole.

Nobody owns your technology. Hence the title.

WHAT THIS BOOK IS

It's a walk through everything your firm pays for. IT support. Cyber. Phones and internet. The website. The marketing. One chapter each, on what's probably wrong with it right now and what it should look like instead. You'll recognise your firm in some of them. Maybe all of them.

Then it's one idea. That all of those things are one thing, and one name should own it.

Then it's three ways to make that true. Do it yourself with the checklists in here. Do it with us, in a course where I show you how. Or have us do it, which is what we do for a hundred firms. And what the first 90 days look like when we do.

WHAT THIS BOOK IS NOT

It's not a memoir. There's a bit of me in here because you should know who's talking, but I'm not the point.

It's not a cyber scare book. You've had enough of those. The threats are real and we'll deal with them properly. But fear is a lousy reason to make a decision and I'm not going to use it on you.

It's not a sales pitch dressed up as a book. If you finish it and decide your current setup is fine, you'll have lost twenty bucks and an afternoon and gained a set of checklists. I can live with that.

ONE MORE THING BEFORE WE START

Everything in here runs on a simple belief, and if you don't buy it the rest won't land.

Technology is the backbone of your firm.

Not a cost line. Not a utility like the water bill. The backbone. The thing that carries your billing, your matters, your client files, your phones, your ability to work from home on a Tuesday because a kid's sick. When it's crook, everything above it limps. And you can't put marketing on top of a crook backbone. You can't automate a mess.

Get the backbone right. Lock it down. Then switch on the growth.

That's the order. That's the book.

Let's go.

PART ONE

What you've got

CHAPTER 1

Technology is the backbone

A few years back we were asked to look at a business that had been living with Outlook crashing for six months.

Six months.

Not a law firm, as it happens. A small trades outfit, five people, four computers and a server in the corner. But the story is the same one I see in firms ten times the size, so bear with me.

Their whole operation ran off the Outlook calendar. Every job, every technician, every site visit. And for six months Outlook had been crashing, prompting for repairs, losing the calendar for an hour at a time. They'd ring their IT guy. He'd fix it for a day. It would come back.

Nobody fixed it because nobody owned it. The IT guy owned the ticket. The owner owned the pain. The calendar, the thing the business actually ran on, belonged to nobody.

When we got under the bonnet the cause was boring. It usually is. But that's not the point. The point is that a business had been limping for half a year on a problem that wasn't an emergency, so it never got fixed. It just got lived with.

That's what a crook backbone looks like. Not a disaster. A limp.

WHAT THE PARTNER SEES

If you run a firm, here's what technology looks like from your chair.

The laptop that takes four minutes to boot. The printer that works for everyone except the one person who needs it at 4:55 on a Friday. Outlook doing something weird. The Wi-Fi in the back meeting room. The phone system that drops the call when you transfer it. The password reset at 8am that eats forty minutes of a paralegal's day.

Individually, none of it is worth a meeting. That's exactly the problem. Each one is a one percent in reverse. A tiny tax on every hour, paid by every person, every day, that never adds up to a number anyone looks at.

Try this. A thirty-person firm. Say each person loses fifteen minutes a day to technology that's "fine". That's seven and a half hours a day across the firm. Thirty-seven hours a week. A full-time person, doing nothing, forever. At professional services rates, you can do the maths on what that costs in billable time. I'd rather you did it than me, because you'll believe your number.

WHAT'S ACTUALLY UNDERNEATH

Now here's what it looks like from my chair.

Under all those small annoyances is a set of things that either work or don't. I call it the backbone, because that's what it does. It holds everything else up.

Identity. Who can log in, to what, from where. Your Microsoft tenant, your user accounts, your multi-factor, your admin rights. If this is loose, everything is loose.

Data. Where your files actually live. SharePoint, a server, someone's desktop. Whether they're backed up. Whether the backup has ever been tested by restoring something. (Most haven't. Ask.)

Devices. Every laptop and desktop. Who manages them, whether they're patched, whether a lost one can be wiped from your phone.

Network. The switches, the Wi-Fi, the firewall, the cabinet nobody opens. Usually installed by whoever was cheapest the year you moved in.

Connection. The line to the internet, and whether it's the right size for what you do now, not what you did in 2019.

Phones. The system, the numbers, who holds the account.

The apps the firm runs on. LEAP, FYI Docs, APS, BGL, Handisoft, MYOB, Xero, your practice management system, your document system. The things that make you a law firm or an accounting practice and not just an office.

That's the backbone. Seven things. Every firm has all seven, whether anyone's looking after them or not.

FROM THE BASEMENT TO THE FRONT

If you're old enough to remember The IT Crowd, you'll remember where the IT department lived. The basement. Two blokes, a broken sign on the door, a phone that answered itself with "have you tried turning it off and on again". Nobody upstairs knew their names. Nobody went down there unless something was on fire.

That wasn't just a sitcom. That was the 1990s and most of the 2000s. IT was a cost. A department you funded because you had to, run by people you hoped not to hear from, in a room you'd never seen. The fax machine mattered more.

It's 2026 and the basement's empty. Technology's at the front of the building now, holding the whole thing up. Your email, your files, your matters, your billing, your phones, your website, your calendar, your security, the way a new client finds you and the way an old one pays you. Take any one of those away for a day and the firm limps. Take the lot away and there is no firm. There's a lease and some furniture.

Call it the backbone, or call it the operating system for the firm. Same thing. The layer everything else runs on, that most firms are still funding like it's the basement.

That's the bit that drives me, honestly. Not the tickets. Putting that layer in properly, all of it, and then watching what happens to a business once it's there. Because it's the same every time. Once the backbone's right, the firm grows. Not because of anything clever. Because for the first time, nothing's holding it back.

WHY "BACKBONE" AND NOT "INFRASTRUCTURE"

Because infrastructure sounds like something you can defer. Roads. Pipes. Someone else's problem.

A backbone is personal. When it's out, you can't do anything. You can't lift, you can't turn, you can't sit at your desk for more than ten minutes. And when it's working you don't think about it at all.

That's the standard. Technology you don't think about.

Not technology that's exciting. Not technology you got a demo of. Technology that holds you up while you do the thing you're actually good at, and never asks for attention.

THE TWO MISTAKES

Firms make one of two mistakes with the backbone, and they're opposites.

The first is treating it as a cost line. Something to be minimised. You go to market every couple of years, get three quotes, pick the middle one, and the brief is "keep it running, keep it cheap". You get exactly what you asked for. A provider who keeps it running, cheaply, and whose entire incentive is to do as little as possible for the fee.

The second is treating it as a project. A big migration. A new system. A six-figure "transformation". Everyone's excited for three months and then it's the new thing nobody owns.

The backbone is neither. It's not a cost to minimise and it's not a project to finish. It's a thing that has to be right, all the time, and get a bit better every quarter, and someone has to be responsible for all of it.

THE GYM

Here's how I think about it, and it comes from training.

You can't get fit by doing one exercise, once. Everyone knows that. You can't get fit by doing one massive session a quarter either, though plenty of blokes my age try. You get fit by doing the boring things, together, two or three times a week, for long enough that it stops being a project and starts being how you live. For me I do Park Runs on a Saturday, Kettlebells on another day, footy training another – combined together every week it has made me feel the fittest I've felt in years.

The backbone's the same. Patching once doesn't make you secure. A new server once doesn't make you fast. Multi-factor on half the firm doesn't make you anything. It's the layers. Patches and backups and MFA and documentation and the cabinet checked and the leavers removed, done together, every week, for long enough that nobody remembers when the laptop took four minutes to boot.

The two mistakes above are the two ways people fail at the gym. The cost-line firm is the bloke who bought the cheapest membership and goes twice a year. The project firm is the bloke who hired a personal trainer for twelve weeks, got results, and then stopped.

One good session won't get you fit. One good project won't fix your backbone. The firms that are in shape are the ones where someone turns up every week.

All of it. That's the bit that matters, and the next chapter is about why nobody is.

THE BACKBONE CHECK

Before you go on, five questions. Answer them honestly, out loud if you have to.

1. Who owns your domain name, and could you prove it in ten minutes?
2. When did someone last restore a file from backup to prove the backup works?
3. If a laptop was left in a cab tonight, who would wipe it, and how would they know?
4. How many people in your firm have admin rights, and why?
5. If your IT provider disappeared tomorrow, where are the passwords?

If you got five clean answers, good. You're in better shape than most firms I meet.

If you got "umm" on two or more, that's not a criticism. It's just where you are. Every firm I've ever reset started there.

And if you're thinking "surely my IT provider has all that sorted", I'd gently ask: have you ever seen it? Because the firms with the worst backbones are almost never the ones with no IT provider. They're the ones with a provider who's fine.

CHAPTER 2

The pointing problem

Here's a ticket that landed on a helpdesk I know well.

An outside consultant, hired by a law firm to “do AI”, asked for a global admin login to the firm's Microsoft tenant. She wanted to pull meeting transcripts into the matter folders. Reasonable idea. Useful, even.

But stop and look at what just happened.

A third party, engaged by the firm, has asked for the keys to the entire kingdom. Global admin isn't a login. It's the ability to read every mailbox, reset every password, change every rule, and delete the lot. And the request came through as a support ticket, like a printer jam.

Who decides whether that's okay?

Not the consultant. She's doing her job. Not the helpdesk. They answer tickets. Not the IT provider, unless someone's told them they're responsible for who gets to touch the backbone. And the partners? The partners didn't know the request existed.

That's the pointing problem in one ticket. Three parties, each doing their bit well, and nobody responsible for the whole.

THE THREE VENDORS

Most firms your size have some version of this cast.

The IT guy. Could be a one-man band, could be a managed services company with a logo and a portal. Looks after the computers, the email, the server if there is one. Measured on tickets closed and how fast the phone gets answered.

The marketing agency. Built the website, maybe runs some Google ads, posts on LinkedIn on your behalf. Measured on traffic, or likes, or a monthly report with a lot of green arrows.

The automation bloke. Set up the CRM, or the online booking, or the thing that sends a welcome email. Often a freelancer. Often brilliant. Often gone.

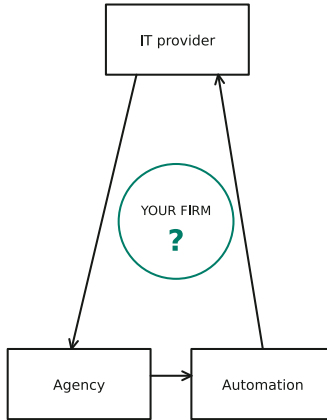
Each one is good at their bit. I want to be clear about that, because I'm not here to bag anyone. I've met excellent IT providers and excellent agencies. The problem isn't the people.

The problem is the gaps between them, and the gaps are where your firm actually lives.

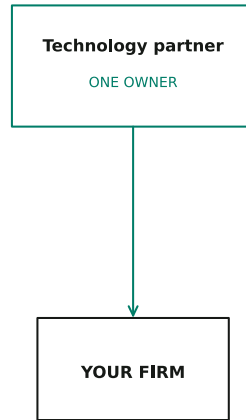
The pointing problem

The gaps belong to nobody. Until one name owns the whole.

FRAGMENTED



ACCOUNTABLE



One accountable partner. A clear route to resolution.

THE POINTING TEST

Five questions. Not for your IT provider. For you.

1. Who owns your domain name? Not who manages it. Whose name is on the registration, and whose credit card renews it?
2. Who owns your Microsoft tenant? Who holds the top-level admin account, and does the firm have it, or does a vendor?
3. Who can log in to your website, and change it, and take it down?
4. Who holds the account for your phone numbers? If you moved phone systems tomorrow, who would port the numbers?
5. Who owns the CRM, the booking system, the automations? Whose login are they under?

If the answer to any of those is a vendor, or “I think it’s the old office manager”, or “umm”, you’ve got the pointing problem.

And I’ll tell you what happens next, because I’ve watched it. The marketing agency rebuilds the website and emails you a login, but the DNS is with the IT guy, so the new site doesn’t go live for a week while two people who’ve never met argue by email. Or the automation sends new enquiries to a mailbox nobody checks anymore. Or someone leaves and the phone account was in their name.

None of those are emergencies. All of them cost you a client, or a week, or a Saturday.

YOU’VE PROBABLY TRIED THE MARKETING ALREADY

Here’s the version of the pointing problem that costs the most, and it’s the one partners bring up last, almost embarrassed.

You’ve tried it. An SEO agency on a retainer for a year. A Google Ads campaign that spent the budget and sent you three enquiries, two of them from recruiters. A new website that looked great at launch and hasn’t rung since. A LinkedIn bloke. A lead-gen company that promised twenty qualified leads a month and delivered a spreadsheet. Maybe all of the above.

And you got something. A bit. Not nothing, which is the frustrating part. Enough to keep paying, not enough to feel like it worked.

Here's what nobody told you. None of it failed because the agency was bad. Most of them weren't. It failed because the agency owned one piece, and the piece they owned sat on top of six pieces nobody owned.

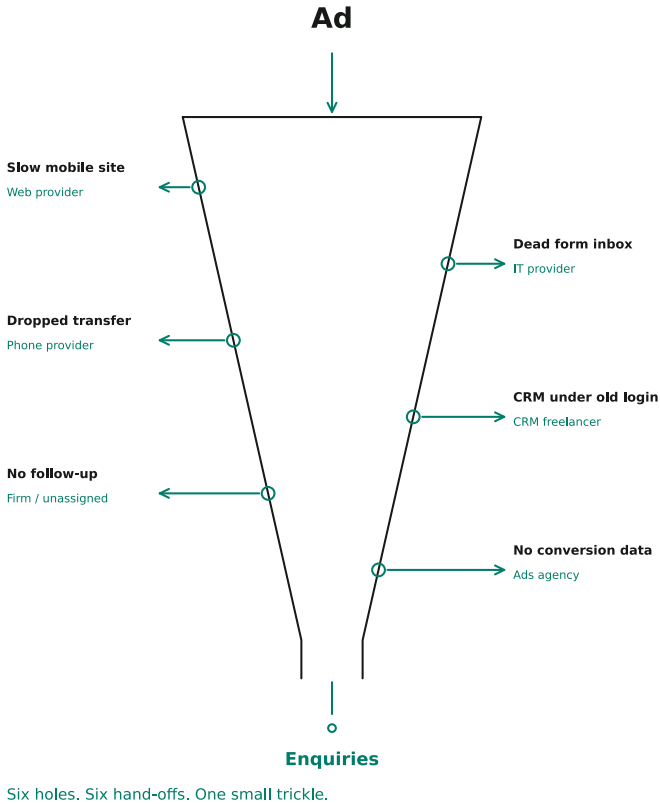
The ad worked. It sent someone to the website. The website was slow on a phone, so a third of them left. The ones who stayed filled in the form. The form went to an inbox the receptionist stopped checking in 2023. The ones who rang instead got the phone system that drops the transfer. The ones who got through never went in a CRM, because the CRM's under a freelancer's login. Nobody followed up, because nobody was told. And at the end of the quarter the agency sent a report with green arrows on it, and you cancelled.

Every one of those gaps is a different vendor. The agency can't fix the phone system. The IT guy doesn't know there's a form. The freelancer's gone.

The marketing didn't fail. It leaked. Out of six holes, and each hole belongs to someone else.

The leak

The ad works. The joins lose the enquiry.



That's what "nobody owns your technology" actually costs. Not downtime. Leads. The ones you paid for and never heard from.

THE ONE NOBODY SAW

One more, because the next few years are going to be full of it.

A firm we look after found their cloud storage filling up fast. Fifty gigabytes and climbing, and nobody had uploaded anything. When we dug in, it was AI agents. Someone had set up a few assistants in a Microsoft tool a while back, and they'd been quietly in-

dexing and copying everything ever since. Nobody knew they existed. Nobody owned them. They weren't malicious. They were just on, forever, because nobody was responsible for the whole.

Every firm is about to have AI tools switched on by someone, somewhere. Some by the IT guy, some by the marketing agency, some by a partner who saw a video. If nobody owns the whole backbone, nobody owns the AI either, and that's a problem I'd rather you solved before it solves itself.

WHY IT HAPPENS

It's not laziness. It's the way the industry's built.

IT companies sell tickets. Response times. Hours of cover. That's what the contract says, so that's what they do. Ask most IT providers what your firm's marketing numbers look like and they'll look at you like you asked a plumber about your tax.

Marketing agencies sell growth. Traffic, leads, brand. Ask most agencies where your backups go and you'll get the same look in reverse.

And automation lives in the middle, built by whoever was around, on top of whatever was there, and it works right up until something underneath it changes.

Here's a small example. A phone system we look after had call transcription built in, running on an AI service from a big-name vendor. One day it stopped. The phone vendor hadn't changed anything. The AI vendor had retired the model it ran on, and the phone vendor's integration wasn't updated yet. Nobody at the firm had done a thing wrong. A feature they relied on just went away, because it was built on someone else's sand.

Automations without a backbone underneath them are built on sand. Every time.

THE STANCE

So here's the opinion, and it's the one that got me into this.

Your IT provider should be measured on growth, not tickets.

I know how that sounds. IT people don't talk like that. But think about what you actually want from technology. You don't want tickets closed fast. You want fewer tickets. You don't want a report on uptime. You want a firm that runs, and a pipeline that fills, and a Friday afternoon where nothing breaks.

Your IT guy has never once been asked about leads. Not because he's useless. Because nobody thought to ask, and he'd have said it wasn't his job.

Personally I reckon it's exactly his job. The website sits on the backbone. The CRM sits on the backbone. The phone that rings when the ad works sits on the backbone. If the person responsible for the backbone isn't also thinking about what sits on top of it, you've got two half-jobs and a gap.

The next five chapters are the gap, one piece at a time. IT support. Cyber. Phones and internet. The website. The marketing. What's probably wrong with each, and what it should look like. Read the ones that sting.

CHAPTER 3

IT support. Tickets, not outcomes

Ring your IT provider right now. Go on. Time it.

If a person picked up inside a minute, knew your firm's name without asking, and could see your laptop on their screen before you finished describing the problem, skip this chapter. You're in good hands.

For everyone else, here's what IT support looks like at most firms I walk into.

WHAT IT LOOKS LIKE NOW

You log a ticket. You get an auto-reply with a number. Sometime later, a person. They ask which computer. They ask you to restart it. It works for a day.

The new starter's first morning is spent waiting for a login that was requested last Thursday. The person who left in March still has an account, still has a licence you're paying for, and nobody's sure if her email's still forwarding somewhere.

Half the firm has admin rights on their own laptop because it was easier that time the accounting software wouldn't update. Nobody can tell you which half.

The server in the cupboard is seven years old. The provider mentioned replacing it two years ago, in a quote nobody actioned. It's fine. It's always fine until it isn't.

There's no documentation. Or there is, in the provider's system, and you've never seen it, and if they disappeared tomorrow the passwords would go with them.

And the monthly report, if there is one, tells you how many tickets were closed and how fast. It never tells you how many tickets there shouldn't have been.

WHY IT'S LIKE THAT

Because that's what you bought. Somewhere back along the line, someone went to market with a brief that said "keep it running, keep it cheap". Three quotes, pick the middle one. And you got a provider who keeps it running, cheaply, and whose whole incentive is to do as little as possible for the fee and charge for the rest.

I'm not having a go at them. That's the deal. Tickets in, tickets out. Hours of cover. Response times in the contract. The industry's built to sell exactly that, and most providers are decent at it.

But it's a half-job. A provider measured on tickets has no reason to reduce them. A provider who doesn't own the whole backbone can't. And a provider who's never been asked about your website, your phones or your leads isn't going to bring them up.

WHAT GOOD LOOKS LIKE

Support that answers. A person, inside a minute, during business hours, with extended and 24/7 options if the firm needs them. Not a bot. Not a form. Not "within four hours".

The person who picks up can see your firm. Your devices, your users, your documentation, your history. They don't ask what company you're from.

The same people over time. The thing partners tell me they hate most is explaining the firm again every time they ring. Good support is built around not doing that.

Fewer tickets, not faster ones. The things that break every week get fixed at the root. Patches land at 2am. Password resets are self-service with multi-factor. The four-minute boot becomes a forty-second one because somebody replaced the drive instead of closing the ticket.

Onboarding and offboarding as a process. A new starter has a login, a laptop, a phone extension and the right software before they arrive. A leaver's access is gone the same afternoon, their licence cancelled, their mailbox handled. Both from one form, not six emails.

Nobody's an admin on their own machine. Including the partners. Especially the partners.

Documentation you can see. Every password, every device, every licence, every vendor, in a portal that belongs to the firm. If the provider vanished, you'd be annoyed, not stranded.

A report a partner reads. Not tickets closed. What broke, what was fixed for good, what was found before anyone noticed, and what's coming up.

Onsite when it's needed, on a schedule that scales with the firm, from someone who knows where the cabinet is.

THE CLEAN SWITCH

The thing partners fear most about changing providers isn't the cost. It's the week. The week where nothing works, the email bounces, the printer vanishes, the practice management system logs everyone out and there's a client at the front desk.

So most firms stay. Not because the provider's good. Because the switch feels worse.

It doesn't have to be. Done properly, your staff shouldn't notice the week happened. Here's the checklist, whether we're doing it or you're making your next provider do it.

- ☐ A handover letter to the old provider, polite, with a date. Most are professional about it. They've been on the other side.
- ☐ Every admin credential, licence detail and backup login collected, and documented if it never was
- ☐ Domain name registered in the firm's name, renewing on the firm's card
- ☐ Microsoft tenant top-level account held by the firm, with a sealed break-glass login, and the new provider as a delegated partner, not the owner
- ☐ Every user account reviewed, leavers removed, unused licences cancelled (this is usually the first saving)
- ☐ Every device under management, patched, encrypted, remotely wipeable, without anyone losing a bookmark
- ☐ One restore performed from backup and screenshotted
- ☐ Network gear opened, documented, and replaced if it's mismatched or tired
- ☐ Internet sized for the firm now, not the firm five years ago
- ☐ Phone numbers in an account the firm controls
- ☐ Every software subscription listed, with its cost and its owner
- ☐ One helpdesk number and email, known to every staff member
- ☐ A monthly report that a partner actually reads

Thirteen things. If your provider did all thirteen when they took you on, you're in better shape than most. If you can't remember them doing any of it, that's the chapter.

And a word on the old provider. Thanks, honestly. They probably did a fair job with the brief they were given. I've never gone into a firm and bagged the last mob, and I'm not going to start in print. Give them the date, let the handover happen, and move on.

CHAPTER 4

Cyber. The baseline nobody set

When I started in IT, 26 years ago, security was three things. Antivirus. Windows updates. Backups. That was most of what an IT person did on the security side, and honestly it was most of what there was to do.

The threats matched. You'd clean the pop-ups off someone's screen. You'd deal with the Blaster worm when it came through in 2003 and rebooted half the office every few minutes. If something got properly wrecked, you'd restore from last night's tape. The bad guys were a kid in a bedroom, or a bloke who'd written a virus to see if he could. Annoying. Rarely ruinous.

It was so much simpler back then.

Now the bad guys run corporate offices. Real ones, with hundreds of staff, payroll, shifts, HR, a sales team and a help desk for their victims. They use AI to write the email that looks like it came from your managing partner. They research your firm online first: who the partners are, who does the payments, who's on leave this week according to LinkedIn, what software you run according to your job ads. They find the hole, and the hole is usually a person with a password and no multi-factor, not a bug in a program.

Back then, most of this was optional. A firm could skip half of it and get away with it for years, because nobody was looking for them.

Now it's mandatory. Not because a law says so, though your insurer and your biggest client will. Because somebody is looking for you, specifically, with a budget.

But the mindset hasn't moved. I still hear it every month, from smart people. "We're too small to be a target. It's the big firms that get hit. Who'd bother with us?"

Here's who'd bother with you. The Australian Signals Directorate took over 84,700 cybercrime reports last financial year. One every six minutes. The average cost to a small business, per report, was \$56,600, up 14 per cent on the year before. For a medium business it was \$97,200, up 55 per cent. [CHECK before print: ASD Annual Cyber Threat Report 2024-25, released October 2025. Update to the current year's figures.]

And the thing hitting businesses most isn't some clever exploit. The top two cybercrimes reported by Australian businesses are email compromise and business email compromise fraud. Together they're a third of everything reported. That's someone getting into a mailbox, usually with a password and no multi-factor, and sending an invoice with their bank details on it to your clients. It doesn't need a big target. It needs one mailbox with no multi-factor, and a small firm with none of the eight is the easiest place to find one.

The big firms have a cyber team, a budget and an insurer who's already made them do the Eight. The criminals know that. So they go where the Eight aren't. A thirty-person accounting practice with trust money, client tax file numbers and a partner who found multi-factor annoying is not too small to be a target. It's the target.

Here's what the old mindset looks like from the inside.

WHAT IT LOOKS LIKE NOW

The insurance renewal arrives with a questionnaire, and there are three questions on it nobody in the firm can answer honestly. So someone guesses. That guess is what gets a claim denied.

Multi-factor is on for most people. Not the partners, because one of them found it annoying and the provider made an exception. The partners are exactly who an attacker wants.

The backups run. Nobody's ever restored anything from them. Nobody knows if they'd work.

An email that was correctly caught by the filter gets released from quarantine, because a staff member asked for it, and asking nicely worked. It was a spoof.

Someone's been pasting client details into an AI tool for six months. Not maliciously. It's useful. Nobody decided whether that was okay, because nobody owns it.

There's a 90-page security policy a consultant sold the firm. Nobody's read it, including the consultant.

And the cyber security "product" your IT provider sells is an add-on. A line item you can tick or not. Which tells you everything about how they think about it.

WHY IT'S LIKE THAT

Two reasons. The first you've just read. The threat grew up and the three things didn't, and most IT providers are still selling the three things, with a couple of extra logos, and calling it security.

The second is that cyber got sold as an upsell, by people who sell fear.

The industry worked out years ago that scaring partners is easier than explaining things to them. So you got the seminars, the ransomware statistics, the quote with "Advanced Threat Protection" on it for an extra \$12 a user. And you either paid it, or you didn't and felt vaguely guilty.

Neither of those is a baseline. And a baseline is what you need. The minimum every firm stands on. Not a tier you can decline. Not an add-on. The thing that's there before anything else gets built, and that nobody thinks about once it is.

At CX we're a cyber-first IT provider. We're not a security firm, that's chapter 9, but we take cyber more seriously than most of the industry, and it shows up as a rule rather than a slogan. There's a minimum baseline we expect every client to be on, it lines up with Level 1 of the Essential Eight, and you can't buy a plan from us that sits under it. It's not always the most popular sentence on a first call. It's the one I'm least willing to move on.

THE ESSENTIAL EIGHT, IN PLAIN ENGLISH

The Australian Signals Directorate, the government's cyber agency, publishes a list of the eight things that stop most attacks. Eight categories. Under each one sits a handful of specific settings, forty-odd across the lot at the first level, and more as you go up. They've been refining it for years based on what actually gets Australian organisations breached, and it's about as close to a straight answer as this industry has. It's not short, exactly. But it's finite, and it's written down, which is more than you can say for most of what gets sold as security.

Each of the eight has maturity levels, zero to three. Level 1 stops the opportunistic stuff: the mass phishing, the commodity malware, the person who found a password on a list. Levels 2 and 3 are for firms that are specifically targeted, or that handle things worth targeting.

Is it the law? For a private firm, no. Federal government agencies have to do it. You don't.

But here's who's going to ask you anyway. Your cyber insurer, at renewal, in a questionnaire that reads like it was written by someone who's read the Essential Eight. Your bigger clients, in a supplier questionnaire, because their insurer asked them. Any tender you go for. And increasingly your own professional body, who'd rather you didn't end up in the paper.

So it's not the law. It's just the test everyone's about to set you. Level 1 is the pass mark.

THE MONDAY MORNING EIGHT

Here's each control as what it looks like at 9am on a Monday, rather than how the government writes it.

1. **Applications get patched.** Chrome, Adobe, Office, Teams, all updated in the background without anyone clicking anything. The "update available" bubble that's been there since March is gone, because it was done at 2am.
2. **Windows gets patched.** Updates install overnight and the machine restarts on a schedule. Nobody has clicked "remind me tomorrow" for six months, because nobody can.
3. **Everyone taps their phone to log in.** Every person. Every system that matters. Including the partners. Especially the partners.
4. **Nobody is an admin on their own laptop.** The person who can install anything is the person who can be tricked into installing anything. Staff can do their jobs without admin rights. We've proven it a few hundred times.
5. **The laptop won't run a program that arrived by email.** A file that's just landed in Downloads doesn't get to execute. The real software you use is allowed. The surprise isn't.
6. **The spreadsheet that "needs macros enabled" doesn't work.** Macros from the internet are blocked. If a supplier's genuine invoice needs macros, that's a conversation, not a click.
7. **The browser doesn't run the old stuff.** No ancient plugins, no ads with code in them, nothing from the last decade that's only still around because nobody turned it off.
8. **Backups run every day and someone checks.** Not "we have backups". Backups that ran last night, that are kept for long enough, that can't be deleted by someone who's got into your email, and that a human looked at this morning.

That's Level 1, in eight lines. Each of those lines is really a handful of settings, and that's where the forty-odd controls live. The settings are the course's job and your provider's job. The eight lines are yours, so you know what the settings are for. Read them again and

notice there's nothing in there a thirty-person law firm can't do. The firms that fail it aren't failing because it's hard. They're failing because nobody owned all eight.

And notice they work together. Antivirus on its own is one exercise. The Eight is a program. Multi-factor stops the stolen password. Patching closes the known hole. No admin rights stops whatever got through from spreading. And backups mean that even when all of that fails, you're back by lunchtime. Take one away and the rest have a gap in them. That's why it's eight and not one, and why it's every machine and every person, not most of them. Half a program is the gym membership you don't use.

THE ONE PERCENTERS

The Eight is the list everyone can quote. It's the program. But anyone who's played footy knows the game isn't won by the stuff in the highlights. It's won by the smother, the shepherd, the chase-down nobody claps for.

Cyber's the same. There's a second list, of boring things that aren't on the Eight, that a cyber-first provider does anyway, on every firm, and checks every week. None of them is impressive on its own. Together they're the difference between a firm that passes the insurer's questionnaire and a firm that looks like Fort Knox to someone scanning the street.

Here's ours. Not all of it, but enough that you'll recognise whether your provider's doing it.

- Email authentication. Three records on your domain, SPF, DKIM and DMARC, set and enforced, so nobody can send email as you. Most firms have one of the three, half done.
- DNS and the website behind Cloudflare, with HTTPS enforced. The site can't be served insecurely, and the records that point everything at everything live somewhere one name controls.
- Disk encryption on every machine. BitLocker on Windows, FileVault on Mac. A lost laptop is a lost laptop, not a data breach.

- A password manager for the whole firm, with shared vaults for the things the firm owns. So the passwords aren't in a spreadsheet called passwords.xlsx, and they aren't in the departed practice manager's head.
- Web filtering on every device, so a bad link doesn't resolve, even on the home Wi-Fi.
- Endpoint detection with a human watching it. Antivirus nobody looks at is just antivirus.
- Email filtering with a quarantine rule. Nothing gets released without a second set of eyes, and the people who can release are the people trained to look.
- Logins blocked from countries the firm doesn't operate in. If you've got no clients in Nigeria, nobody logs in from Nigeria.
- Alerts on suspicious logins and on any account without multi-factor, so the partner exception gets found in a day, not at renewal.
- Mailbox forwarding rules checked. A quiet forward to an outside address is the classic sign someone's already in.
- Leavers offboarded the same day. Sessions revoked, licences cancelled, forwarding checked, not "we'll get to it Friday".
- Anything facing the internet scanned from outside, on a schedule, so an open port gets found by us before it gets found by someone else.
- Short, regular security awareness training, with a fake phishing email now and then. Not a one-off video from 2022.

Thirteen things. None on the Eight. All on our list.

Each one is a one percenter. Nobody's going to put "enforced DMARC" in a brochure. But done together, on every machine, every week, they're what makes a thirty-person firm not worth the criminal's time, and that's the whole game.

SAY THESE WORDS

You're not going to set any of this up yourself, and you shouldn't. But you should be able to say the words in a meeting. Hand the Eight and the thirteen to whoever looks after your IT and ask them to show you each one. Not tell you. Show you, on a screen.

If they can show you all of it inside ten minutes, you're in good hands. If they can't, you've learned something, and it wasn't about the software. How to set each one up, step by step, is in the course. This book's job is to make sure you know what to ask for.

THE FIVE PAGES

You need five policies, one page each, in words a new starter could read on their first morning and actually follow. Not the 90-page thing.

Acceptable Use. What staff can and can't do with the firm's technology. Personal email, personal devices, what gets installed, what gets shared, and what happens if a laptop goes missing.

Passwords and Multi-Factor. Everyone uses the password manager. Nobody reuses a password. Multi-factor on everything. No exceptions for seniority, because seniority is exactly what attackers go for.

Incident Response. What a staff member does in the first ten minutes if something looks wrong. Who they call. What they don't touch. One page, on the wall, because at the moment it matters nobody's going to open a folder.

Devices and Working Away. Which devices can touch firm data. What's required on a personal phone that gets email. What working from the kitchen table looks like, properly.

AI Use. New, and now the most important page of the five. Which AI tools are approved. What can and can't be pasted into them. Client names? Matter details? Financials? Who in the firm owns AI, so the next tool somebody switches on gets noticed.

The firms that ban AI will lose staff and lose work to the firms that didn't. The firms that don't own it will end up in the paper. One person, usually a partner or the practice manager, owns which tools are approved and what goes in them. That's the whole policy.

DAY ONE OF A BREACH

Even with all of the above, something can still get through. The point of the baseline isn't that nothing ever happens. It's that when something does, it's small, it's contained in an hour, and you know exactly what to do.

In the first hour, contain it. The affected account gets its sessions revoked and its password reset. The device gets isolated from the network with a click. Admin access gets checked. Nothing gets deleted, because the evidence matters.

In the first four hours, work out what actually happened. One mailbox, or ten? Did anything leave? Was a rule set up to forward email quietly, which is the classic move? A plain-English summary, not a log file.

On day one, the insurer gets told, because most policies require prompt notice. And someone works out whether the Privacy Act's Notifiable Data Breaches scheme applies. For most firms over the turnover threshold, and for health providers at any size, it does. If personal information has been accessed in a way likely to cause serious harm, there's a process for notifying the regulator and the people affected, and it runs on a clock.

And the quarantine story from the top of the chapter? The fix wasn't blaming anyone. The fix was a rule: nothing comes out of quarantine without a second person checking, and the people who can release are the people trained to look. Process beats memory. Every time.

WHY IT'S A BASELINE, NOT A TARGET

Level 1 is where every firm should start, and it's where every CX client sits, no exceptions. Some need more. If you hold client money,

immigration files, medical records, or you're the kind of practice that gets named in a dispute, you want Level 2, and anyone looking after you properly will say so.

But I'd rather every firm in the country was solidly at Level 1 than a handful were at 3 and the rest were at nothing. The baseline is the point. Get everyone on it. Then raise it.

CHAPTER 5

Phones and internet. The cable in the wall

Nobody writes a chapter about phones and internet. It's the water bill. It's the thing you set up when you moved in and haven't thought about since.

Which is exactly why it's the most neglected thing in the firm, and why I'm giving it a chapter.

WHAT IT LOOKS LIKE NOW

The internet plan was picked in 2019 for twelve people. There are thirty-eight now, all on Teams calls, all on a cloud practice system, all syncing to SharePoint. Every afternoon around three it crawls, and everyone's learned to live with it. Nobody's connected the crawl to the plan.

The phone system was installed by a phone company who've since been bought by another phone company. The transfer button drops the call about one time in four. The receptionist's learned which extensions to avoid.

The main number is in the old practice manager's name. She left in 2022. Nobody's noticed because the bill still gets paid.

After 5:30 the phone goes to a voicemail that someone checks on Monday. A prospect who rang at 5:45 on a Thursday with a letter from the ATO in their hand has rung three other firms by then.

Nobody knows how many calls were missed last month. Nobody knows how many rang, got the voicemail, and hung up. There is no number for that, because the phone system doesn't talk to anything.

When the internet drops, you ring the IT guy. He says it's the ISP. You ring the ISP. They say the modem's fine, it must be your network. You ring the IT guy. He says they always say that. Two hours. Nobody owns the cable in the wall.

And the thing with the call transcription that stopped working one day? That was in chapter 2. It was built on someone else's sand.

WHY IT'S LIKE THAT

Because phones and internet sit between two vendors who both think it's the other one's job. The IT provider thinks connectivity is a utility, like power. The carrier thinks everything past the modem is IT. And the phone system is a third mob altogether, who'll support their handsets and nothing else.

So the firm ends up with three accounts, three bills, three support numbers, and the person who understands how they fit together left in 2022.

WHAT GOOD LOOKS LIKE

The connection is sized for the firm now. Business-grade fibre where you can get it, with a backup path so a dug-up cable on the street doesn't take the firm offline for a day. Reviewed every year as the headcount changes, not every time it crawls.

The phones are a cloud system, not boxes on the wall. Extensions scale with people. Staff answer from a laptop or a mobile with the firm's number, which means working from home is working, not a workaround. Transfers don't drop. Call queues exist. Voicemails arrive as transcribed emails.

The numbers belong to the firm. In the firm's name, in an account the firm controls, documented, so they can be ported anywhere in a week.

Missed calls get a text within a minute. "Sorry we missed you, how can we help?" Sounds trivial. It's the single highest-return thing in this chapter, because a prospect who gets a text doesn't ring the next firm.

After-hours has an answer. A person, an answering service, or an AI assistant that takes the details and books a time. Not a voicemail checked on Monday.

The phone talks to the CRM. Every call logged against a name. Every new caller a lead. Someone can tell you how many calls came in last month, how many were missed, and what happened to the ones who rang about a new matter.

And there's one number to ring when any of it breaks. Internet, phones, Wi-Fi, the lot. The person who picks up can see the connection, the modem, the phone system and the network from one screen, and doesn't get to say "that's the carrier".

THE THING PARTNERS MISS

Phones and internet aren't a utility. They're two things at once.

They're how clients reach you. The phone is still how most professional services clients first make contact. If it rings out, or drops, or goes to voicemail, nothing the marketing agency does matters.

And they're what everything else runs on. Every cloud system the firm uses, every Teams call, every backup, every AI tool, is only as good as the connection under it. A crook connection makes every other piece of technology look broken, and every vendor blame every other vendor.

One owner. One number. The cable in the wall is part of the backbone. Treat it like one.

CHAPTER 6

Websites. The brochure

Pull up your firm's website on your phone. Not your laptop. Your phone, because that's where most of your prospects will see it. Now be honest.

It takes four seconds to load, and the first thing you see is a stock photo of a handshake. There's a paragraph about your values. There's a page of partners with photos from the last rebrand. There's a Contact Us page with a form.

That's a brochure. Printed in 2019 and never reprinted.

WHAT IT LOOKS LIKE NOW

Here's what's missing, and it's the same list at nearly every firm I look at.

No number you can tap. The phone number's in the footer, as text, and tapping it does nothing.

No way to book. A prospect who's ready to talk has to fill in a form and wait for someone to ring back. Most won't wait. They ring the next firm on the list.

No chat. Nobody there at 8pm when the bloke who just got the letter from the ATO is searching. No AI assistant to answer the first three questions and book the call.

No call to action, or the wrong one. "Learn more". "Contact us". Nothing that says what to do next and why now.

No reviews on the page. Eleven on Google, none where the prospect is actually looking.

The Google listing is half done. Old hours. Two photos. Services not listed. The category's wrong. Nobody's replied to a review since 2022.

Nothing on the site answers a question. Your prospects type "do I need a lawyer for a boundary dispute" or "how much does an SMSF audit cost", and your site has a page called Services that lists nouns. Search engines, and now AI assistants, name the firms that answer. You're not one of them.

Nobody knows what happens when the form is submitted. Try it. Submit your own form and time how long until a human responds. I've done this with partners sitting next to me and watched their face.

No tracking. Nobody can tell you how many people visited last month, what they did, or where they came from. So nobody can tell you whether the agency's work did anything, which is why the report has green arrows instead of numbers.

Nothing's connected. The site doesn't talk to the CRM. The CRM doesn't talk to the phone. The phone doesn't talk to anyone.

And underneath all of it: nobody knows where the site is hosted, who has the login, when the SSL certificate expires, or what happens if the web guy's number stops working. The domain's with IT. The hosting's with the web guy. The content's with the agency. The form goes to a mailbox IT set up and the agency forgot about.

Ten things missing. Not one of them is expensive. Every one of them is a different vendor's job, which is why they're all missing at once. The web guy built a brochure because that's what he was asked for. Nobody asked for a website that rings, because nobody owned the ringing.

WHY IT'S LIKE THAT

Because websites get bought as a project. Every four or five years someone decides the site looks dated, an agency gets a brief and a budget, there's a launch, everyone's pleased, and then nobody touches it until the next rebrand.

A website isn't a project. It's open 24 hours a day, it's where most prospects meet you first, and it needs someone checking it the way you'd check the phones. Not a redesign every five years. A look every month at whether it rang.

WHAT GOOD LOOKS LIKE

Fast on a phone. Under two seconds. That alone keeps a third of your visitors who currently leave.

A number that taps to call. A booking link that works, so a prospect can pick a time without waiting for anyone. A chat on the page that's answered, by a person in hours or by an AI assistant that knows the firm's rules at 8pm. And every enquiry, whichever way it came in, landing somewhere a human sees it inside minutes.

One clear ask on every page. Book a time. Call now. Get the checklist. Not "learn more".

Reviews on the site, pulled live from Google, with the number and the recency where the prospect's eye lands.

A Google Business Profile that's complete. Every service, the right category, current hours, photos of actual people, and every review replied to within a week. For most firms this one listing brings in more enquiries than the website does, and it's free.

Pages that answer questions. The thirty or forty things your prospects actually type, each with a plain-English answer and a next step. That's what search engines rank now, and it's what AI assistants read when someone asks them to recommend a firm.

Tracking that a partner can read. Visits, where they came from, what they did, how many became enquiries. Six numbers on a dashboard, not a 40-page analytics export.

And the plumbing owned by one name. Domain, DNS, hosting, SSL, the form routing, the chat, the CRM connection. So when the agency does good work, it lands, instead of leaking.

THE BROCHURE TEST

Ten minutes, on your phone, right now.

1. Does the number tap to call?
2. Can you book a time without filling in a form?
3. Is there someone, or something, to talk to right now?
4. What's the one thing the home page asks you to do?
5. How many reviews are on the Google listing, and when was the last one?
6. Submit the form. Start a stopwatch.

Six good answers and you can skip the next chapter. In eight years, nobody has.

CHAPTER 7

Digital marketing. The leak

Our own website got hit by a Google update.

I'm telling you that up front because an IT company with a chapter about marketing should probably admit its own traffic fell off a cliff once. It did. One of those core updates Google pushes out a few times a year rolled through, and the site we'd built, the one that had been bringing in enquiries for years, dropped like a stone. Pages that used to rank on the first page were gone.

Nobody had done anything wrong. The rules changed, the way they do.

What happened next is the reason this chapter exists. We treated it the way we'd treat a backbone problem. We found out what actually changed. We rebuilt the content around what people and, increasingly, AI search engines were actually asking. We measured it weekly. And it came back, differently and better, because this time the whole thing was built on purpose instead of by accident.

WHAT IT LOOKS LIKE NOW

You've tried it. Chapter 2 had the list. The SEO retainer. The Google Ads. The new website. The LinkedIn bloke. The lead-gen mob with the spreadsheet. You got a trickle, and a report with green arrows, and you cancelled.

Here's the same picture from inside each piece.

Search. The agency “did SEO” for a year. Blog posts nobody read, about topics nobody searched for, written to a keyword list from 2021. Then Google changed the rules and the little ranking you had went with it. Meanwhile your prospects stopped typing into Google and started asking an AI assistant “who’s a good family lawyer in Geelong”, and the assistant named three firms, none of them you, because your site doesn’t answer anything.

Ads. The campaign ran. The budget went. The clicks landed on the brochure from chapter 6, and a third of them bounced before the page loaded. The ones who stayed filled in a form that went to the inbox nobody checks. Cost per enquiry: unknown, because nobody connected the ad spend to the enquiries. So it got switched off, and the agency blamed the market.

Reviews. Hundreds of happy clients over the years. Eleven reviews on Google. Four of them from 2019. One from a bloke who was annoyed about parking. Nobody’s ever asked a client for a review, because it feels awkward, and nobody’s built the system that does the asking so it isn’t.

Social. Someone posts on LinkedIn when they remember. A Facebook page with the old logo. Posts about the firm’s values that get four likes, three from staff. No one can tell you if a single client has ever come from it.

The CRM. There is one, or there was. It’s under the freelancer’s login. Half the firm uses it, half uses Outlook, and the new enquiries from the website don’t go in it at all. So nobody can tell you how many enquiries came in last month, where they came from, or what happened to them.

Follow-up. The prospect who rang on Tuesday and said “I’ll think about it” was never rung back. Not because anyone decided not to. Because nobody was told to, and nobody owns the follow-up.

And the report. Monthly, from the agency, with impressions and sessions and bounce rates and green arrows. Not one number on it that a partner can connect to a new client.

WHY IT'S LIKE THAT

Because marketing got bought in pieces, from people who each own one piece, and every piece leaks into the next.

The SEO mob can't fix the site speed, that's the web guy. The web guy can't fix the form routing, that's IT. IT doesn't know there's a CRM. The ads bloke can't see what happened after the click. Nobody owns the follow-up, so nobody does it.

You didn't buy bad marketing. You bought six good pieces with no one owning the joins. And the joins are where the leads went.

WHAT GOOD LOOKS LIKE

Switched on, not run as a campaign. Seven things, in roughly this order, each of them sitting on a backbone that can carry it.

The Google listing, complete. Every service, the right category, current hours, real photos, reviews flowing in and replied to. For most firms this is the highest-return hour of marketing work there is.

The website made to ring. Chapter 6. Fast, tap-to-call, bookable, a chat that's answered, one clear ask, and every enquiry landing in front of a human in minutes.

Reviews on a system. When a matter closes or a return is lodged, the client gets a short, polite message with a link. It runs itself. Within a quarter the number's doubled, and the next prospect who Googles you sees it.

Found by search and by AI. Thirty or forty pages that answer the questions your prospects actually ask, in plain language, with a next step. That's what ranks now, and it's what an AI assistant reads before it names a firm. Not blog posts. Answers.

The CRM, live and owned. Every enquiry from every channel, in one place, with a name against it and a next step. Under the firm's login. Backed up like everything else.

Follow-up that happens. The "I'll think about it" prospect gets a text on Thursday and a call the week after, because the system told

someone to. Missed calls get a text in a minute. Quotes that go quiet get chased.

Ads, if they make sense. Not every firm needs them. If you do, they go to a page built to convert, with a number, a form and a chat that are all working because of the six things above, and the cost per enquiry is a number someone can read.

ON THE BUZZWORDS

You'll have heard the new ones by now. GEO. AEO. Generative engine optimisation, answer engine optimisation. Getting your firm named by ChatGPT and by the AI summary at the top of a Google search.

Here's my take, and I've earned it the expensive way. I've bought the GEO course. I've opted into the AEO plan. Nothing changed.

Because it's SEO in disguise. An AI assistant doesn't have a secret source. It reads websites, the same ones Google reads, and it names the firms whose pages actually answer the question that was asked, clearly, with the firm's name and suburb and services stated in plain sentences. That's not a new discipline. That's SEO done properly, which almost nobody was doing, because the agency was writing blog posts to a keyword list instead.

I'll be fair about it. There's a small shift in what matters. The AI cares more than Google used to about your firm being described the same way everywhere, name, location, services, on the site, the Google listing and the directories. It prefers pages that answer a question in the first paragraph over articles that get there eventually. It weights whether other sites mention you. And it leans on reviews, more than ever. That's real. It's also about ten per cent of the job, and any competent SEO person made that shift already.

Nobody needs a separate plan for the ten.

So get the fundamentals right and the AI follows. A fast site. Pages that answer the forty questions your prospects actually ask. A complete Google listing. Reviews that are recent. Who you are, where you are and what you do, written so a machine can read it.

Do that and you'll show up in the AI answers, because that's where the AI gets its answers from.

Which brings me to the guarantees.

"We get you leads, guaranteed." "Twenty qualified enquiries a month or you don't pay." "Rank on page one in 90 days." You'll have seen the ads. Some of them will have found you through this book, which is a bit ironic.

Don't get sucked in. It's marketing fluff, all of it. Nobody can guarantee what Google does next quarter, what the AI assistants name, or whether the people who ring you are worth ringing back. The ones who promise leads either count anything with a phone number as a lead, or they lock you into a term long enough that the guarantee's expired before you've worked out it didn't happen. I've been on the wrong end of that too.

What can be guaranteed is the work. The site's fast. The pages answer the questions. The listing's complete. The reviews are flowing. The Six Numbers are on a dashboard where you can see them move, or not. Pay for the work, not the acronym, and not the promise.

We check how your firm shows up in AI search as part of the Snapshot, and we do it because it's the same check as the SEO one, not because it's a different product.

THE SIX NUMBERS

A partner shouldn't have to read a marketing report. A partner should look at six numbers once a month, next to the ticket count and the backup status.

1. Enquiries this month. How many people asked for help.
2. Where they came from. Google, referral, ads, the website chat, a review.
3. Response time. How long until a human got back to them. Minutes is the target. Hours is normal. Days is where the money goes.
4. Conversion. How many enquiries became a consult, and how many consults became a client.
5. Reviews. Total, and how many in the last 90 days, because recency is what Google and prospects look at.
6. Cost per enquiry. What you spent on marketing, divided by number one.

That's it. Six. If those are moving the right way, the marketing's working. If they're not, you know which of the seven things above to look at.

The agency can't give you these six numbers. Not because they're hiding anything. Because four of the six live in systems they don't own. The phone, the CRM, the form, the follow-up. That's the chapter.

AUTOMATE THE REST

Once the backbone's fixed, the baseline's in and the marketing's switched on, you've got a system with real data running through it. That's when automation stops being a party trick and starts being useful.

New client onboarding, where the engagement letter, the welcome email, the file setup and the first meeting all happen off one trigger. Appointment reminders that cut no-shows. Follow-ups on

quotes that haven't been answered. The monthly "here's where your matter is at" email that clients love and staff never get around to. Internal stuff too: a new starter's accounts, licences and device created from one form.

Two or three to start. Not twenty. Two or three that save real hours, built on a backbone that won't move underneath them, with an owner. Then more each quarter.

The AI assistant on your website is one of these, and I'll say what it is and isn't. It knows your services, your hours, your rules. It qualifies an enquiry and books a time. It does not give legal or financial advice, it does not quote, and it does not pretend to be a person. Done right, it's the best receptionist you've never hired. Done without an owner, it's the AI agents from chapter 2, quietly eating your storage.

That's the four pillars, one at a time. IT. Cyber. Phones and internet. Website. Marketing and automation. Each one probably a bit broken, each one owned by someone different.

Part two is why that's getting worse, and the one idea that fixes it.

PART TWO

Why it's broken, and what fixes it

CHAPTER 8

Why this isn't working anymore

Here's the thing. The three-vendor setup was always leaky. It leaked in 2015 and it leaked in 2019. But it leaked slowly, and a decent firm could live with it, the way the trades outfit in chapter 1 lived with Outlook crashing.

Five things have changed in the last few years, and together they've turned a slow leak into a fast one. If you've felt like technology got harder to manage lately, you're not imagining it. Here's why.

1. AI TURNED UP, EVERYWHERE, OWNED BY NO ONE

Two years ago AI was a thing you read about. Now it's in Word, in Teams, in your practice management system, in your phone system's transcription, on your staff's phones, and in whatever tool the marketing agency just started using.

Every one of those was switched on by someone. None of them were switched on by the same someone. The IT guy enabled Copilot because Microsoft nagged him. A partner started using ChatGPT because her son showed her. The agency's using an AI writer. The phone vendor's transcription runs on a model that got retired last month.

Meanwhile your prospects stopped Googling and started asking an assistant to recommend a firm. The assistant reads websites that answer questions. Yours lists nouns.

AI without an owner is the pointing problem with the volume turned up. More tools, more logins, more places for client data to go, and more things that quietly stop working when the model underneath changes. The firms that handle this well won't be the ones that banned it. They'll be the ones where one name owns it.

2. THE INSURERS STARTED ASKING

Five years ago cyber insurance was a form with four questions. Now it's a questionnaire that reads like the Essential Eight, and the answers are checked, and a wrong one voids the policy.

And it's not just insurers. Your bigger clients send supplier security questionnaires, because their insurer asked them. Tenders ask. Professional bodies ask. The regulator asks after a breach.

The test used to be optional. Now it gets set for you, on a date you don't choose, and the three-vendor setup can't answer it, because the answers live in three places and nobody can see all three.

3. GOOGLE MOVED THE GOALPOSTS, AND THEN AI MOVED THEM AGAIN

The brochure website worked, sort of, for a decade. Google rewarded a page per service and a blog nobody read. Then the core updates started rolling through two or three times a year, each one flattening sites that didn't actually answer anything. Ours got flattened. It's in chapter 7.

Then AI search arrived on top. Now a prospect asks an assistant and gets three names. The assistant isn't reading your stock photo of a handshake. It's reading whether your site answers the question that was asked.

The agency that built the brochure didn't do anything wrong. The rules changed, twice, and nobody at the firm owned keeping up.

4. THE OFFICE STOPPED BEING THE OFFICE

Hybrid work made the backbone the office. The kitchen table is a workstation. The home Wi-Fi is the network. The laptop in the car is the server room.

That was fine when IT, cyber, phones and internet were four separate things in one building. It's not fine when they're four separate things across thirty buildings. Who manages the laptop at home? Who filters the home Wi-Fi? Whose job is it when the phone app doesn't ring on the mobile? Four vendors, thirty locations, and the gaps multiply.

5. THE TOOLS MULTIPLIED

Ten years ago a firm ran on a server, Office and a practice system. Now it's thirty cloud subscriptions, each with its own login, its own admin, its own data, its own bill, and its own vendor who'll support their bit and nothing else.

Nobody has a list. When we do the handover in the first week, the software list is the thing that shocks partners most. Not the cost, though the cost is usually a surprise. The number. Thirty things, and the firm couldn't name fifteen of them.

Every one of those is a place for the pointing problem to hide.

WHAT THAT ADDS UP TO

The old model, three vendors and a partner in the middle, was built for a world where technology was one building, a handful of systems, and a threat level you could ignore. That world's gone.

Now there are more tools, in more places, with more people asking you to prove they're secure, and AI switched on across the lot by whoever got there first. The joins between vendors used to be a slow leak. They're now where the firm's time, money and leads go.

You can't fix that by finding a better IT guy, or a better agency. They'll still be two people who've never met, with a gap between them.

You fix it with one idea. Next chapter.

CHAPTER 9

How CX365 brings it all together

Picture an iceberg.

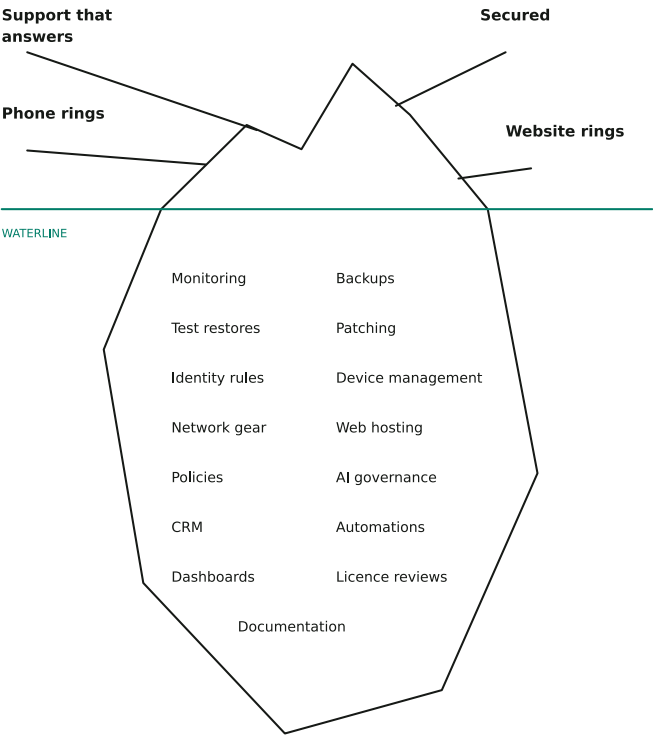
Above the waterline is what you see as a client. Support that answers. Technology that's secured. A phone that rings and a website that rings. A budget that doesn't surprise you. That's it. That's all a partner should ever have to think about.

Below the waterline is everything that makes the top part true. The monitoring. The backups and the test restores. The patching. The identity rules. The network gear. The policies. The CRM. The automations. The dashboards. All of it running, all the time, so you never have to look down.

The five chapters you've just read are what it looks like when the bit below the waterline belongs to five different people. This chapter is what it looks like when it belongs to one.

The iceberg

What you see is supported by what you never have to think about.



One owner above and below the waterline.

ONE OWNER

Here’s the idea. It’s the only idea in the book, really. Everything else is detail.

One name owns all of it.

Not one name per piece. Not “IT does the first two and the agency does the website and we’ll see about the phones”. One person, or one firm, who’s responsible for the backbone and everything that sits on it, and who you’d ring about any of it.

The test is the Pointing Test from chapter 2. Ask “who owns our domain, our tenant, our website, our phones, our CRM, our AI?” If it’s one answer, you’ve got an owner. If it’s six, you’ve got the pointing problem.

When one name owns it, the leaks close. The ad lands on a fast site because the same people own both. The form goes to a human because the same people own the form, the inbox and the CRM. The phone talks to the CRM because the same people set up both. The AI tool gets noticed because the same people own the tenant. The insurer’s questionnaire gets answered in an afternoon because the answers are all on one screen.

None of that is clever. It’s just what happens when nobody has to ring someone else.

ALL YOUR EGGS IN ONE BASKET

I know what you’re thinking, because every partner says it at about this point.

“Isn’t that putting all our eggs in one basket?”

It’s good advice, most of the time. Don’t put your super in one stock. Don’t have one client who’s half your revenue. Spread the risk.

It’s the wrong advice for technology, and here’s why.

The eggs are the products. Microsoft for email and files. A phone system. An internet carrier. A website host. A CRM. A backup system. Those should absolutely be in different baskets, and at a firm we look after they are. If Microsoft has a bad day, the phones still ring. If the carrier digs up a cable, the backups still run. That’s the diversification, and it’s built in.

What you don’t want is a different farmer for every basket.

That’s what most firms have got. One bloke looks after the Microsoft basket. A different mob looks after the phone basket. A third checks the website basket once a year. Nobody’s looking after the backup basket at all, they just assume someone is. And when a fox

gets in, which it does, every farmer says the fox came through someone else's fence.

One farmer. Many baskets. The farmer knows what's in every one, checks every one on the same walk, and when something's wrong there's exactly one person to ask. That's not concentration risk. That's the only way a fox gets noticed.

It's also the honest answer to "what if you get hit by a bus". The baskets are yours. Your domain, your tenant, your numbers, your data, documented and in your name, in a portal you can see. If the farmer vanished tomorrow, the next one could pick up the walk in a week. The firms that are actually exposed are the ones where the domain's in the web guy's name and the passwords are in the old practice manager's head. That's eggs in a basket nobody can find.

And one carve-out, because it's a fair one. You might keep a marketing person. Someone who writes your content, runs your LinkedIn, does your brand. That's fine. That's creative work, and a good one is worth keeping. What they shouldn't own is the basket. The domain, the DNS, the hosting, the form routing, the CRM, the phone, the backbone under all of it. That's one farmer's job, and when it is, the marketing person's work finally lands instead of leaking.

ONE PLATFORM

For us, the one name is CX IT Services, and the thing we own it with is a platform we built called CX365.

I want to explain why we built our own, because it matters.

Most IT providers rent their tools. A ticketing system from one vendor, monitoring from another, backups from a third, documentation from a fourth. Each one a logo on an invoice you never see. It works. It also means your provider can't show you the inside of anything, because they don't own it. They're looking at someone else's dashboard too.

We got sick of that. So over the past few years we built our own.

A portal where a firm sees its tickets, its devices, its users, its backups, its documentation, its policies, its AI usage and its marketing numbers, in one place. Yours, from day one.

A monitoring box at each site, which we call the Beacon, that watches the network from the inside and reports back.

Backups we run ourselves, on infrastructure we control, with the data staying in Australia.

The security monitoring, the web filtering, the device management, the password manager, built in. Not add-ons.

The CRM, the automation platform, the website chat, the reviews engine, the missed-call text-back, the Six Numbers dashboard, all on the same platform, all talking to each other, because they were built to.

And on a call with us, we share the screen and show you the inside. The actual backup job. The actual patch status. The actual numbers. No other IT provider I know of can do that.

CLIENT ZERO

We run every bit of it on ourselves first.

The AI assistant that answers our website chat and books our calls is the one we'll put on yours. The reviews system runs on our own clients. The website recovery in chapter 7 was ours. The Six Numbers are on my dashboard, and I look at them on the first of every month, and some months I don't like them, and that's the point. The Five Pages in chapter 4 are the ones our own staff sign. The Beacon is in our own office.

If it doesn't work for us, it doesn't ship. I'm the first client of everything in this book, and the most demanding one.

WHO'S TALKING

You should know who's saying all this.

I've been in IT for 26 years, most of it inside professional services firms. Law firms, accounting practices, medical clinics, financial

planners. Places where the software has names like LEAP and FYI Docs and APS and BGL and Handisoft, and where the practice runs on it the way a hospital runs on power. I know those systems from the inside, at 7am on the day the end-of-year rollover didn't go through.

Nearly eight years ago I left a steady job at a decent IT company and started CX. Ever since i was younger i always wanted to run my own business. Working with 100s of other businesses i loved helping them grow. I didn't start it to be another IT provider. There were plenty. I started it because I'd watched the industry sell tickets for two decades and I thought businesses deserved something else.

Today we look after more than a hundred professional services firms across Australia and New Zealand. Melbourne's home, Level 6 on Bourke Street, but our clients are in every state and across the Tasman. We're an accredited partner of the Australian Signals Directorate's cyber security program, which is the thing that lets us talk about the Essential Eight with a straight face.

I'm not a marketer, and I'm not a cyber security firm. I'm what i like to call your technology partner. One of a very small number in this country who'll take responsibility for all of it, under one roof, on one platform.

Nobody owns your technology. We'd like to. The next chapter is what "all of it" actually means.

CHAPTER 10

The four pillars, and the order they go in

“All of it” needs a shape, or it’s just a long list. Here’s the shape.

THE FOUR PILLARS

Everything a firm pays for in technology falls into one of four. These are the four things one name has to own.

Technology and IT. The backbone from chapter 1. Identity, data, devices, network, connection, phones, the apps the firm runs on. Chapters 3 and 5 were this pillar: the support, and the cable in the wall.

Cyber security. The baseline under the firm. The Essential Eight, the Five Pages, the insurer’s questionnaire answered honestly, an owner for AI. Chapter 4.

Digital marketing. The part that brings clients in. The Google listing, the website that rings, the reviews, being found by search and by AI, the ads if they make sense, and the Six Numbers. Chapters 6 and 7.

Automation. The repetitive stuff, done by the system. Onboarding, reminders, follow-up, missed-call text-back, the AI assistant on the site, the new-starter form. The end of chapter 7.

Four pillars. Most providers own one. A few own two. The whole argument of this book is that they're not four things. They're one thing with four sides, and the gaps between them are where your time, money and leads go.

FLIPPING THE INDUSTRY

Here's a test you can run tonight. Go to the website of any IT company in the country and look for the word "marketing". You won't find it. Now go to any digital agency's website and look for "security", or "backups", or "Microsoft". Same result.

It's not an accident. The IT company thinks marketing is fluffy and doesn't want to be blamed when the ads don't work. The agency thinks IT is plumbing and doesn't want to be blamed when the email goes down. Each of them has decided, quite deliberately, that the other half is someone else's job.

And that's exactly where the leaks are. Not inside either one's patch. In the gap between them, where the form goes to a dead inbox and the domain's in nobody's name and the AI tool got switched on by whoever got there first. Nobody owns the gap, because both of them have agreed it isn't theirs.

We want to flip that. Not improve it. Flip it.

Because here's what I reckon a firm your size actually needs, and it's shorter than the list you've currently got. You don't need a digital marketing company. You don't need an IT company. You don't need a phone company, an internet company, a web host, an email provider, a backup vendor and a bloke who does the CRM. You don't even need a managed IT services provider, which is what the industry calls us and what I've spent eight years trying not to be.

You need a technology partner. One. Whose job is to help your business grow by managing everything with a plug, a login or a password, and who's measured on whether the firm's growing, not on how many tickets got closed.

That's the flip. Instead of six vendors who each own a slice and nobody owning the joins, one partner who owns the lot and is accountable for the result. It's not a new kind of IT company. It's a different job, and as far as I can tell almost nobody's doing it, because it means an IT bloke has to learn marketing and an agency has to learn security, and neither of them wants to.

We did. That's the whole business.

WHY THEY'RE EQUAL

I get asked which pillar matters most. The honest answer is that it depends which one's broken this week.

But I'll say this. The industry treats cyber as the serious one and marketing as the fluffy one, and I think that's exactly backwards for a firm your size. Cyber is a baseline. Once it's in, it's in, and it mostly just needs checking. Marketing is the thing that pays for everything else. A firm with a perfect security posture and no new clients is a very secure way to go broke.

So: four pillars, treated as equals. Cyber's the deepest, because we're accredited for it and because the insurer will ask about it first. But it's not the identity. The identity is technology partner. All four.

THE THREE PHASES

The pillars are what gets owned. The phases are the order you do it in, and the order matters more than most people think.

Assess. Before anything gets fixed, find out what you've actually got. Who owns the domain, the tenant, the numbers, the website, the CRM. What's on the software list. What the backups actually do. What the outside world sees. You can't fix what nobody's written down, and at most firms nobody has.

Fix and Secure. The backbone made right, then locked down. Devices managed, identity tightened, network documented, backups proven, internet sized, phones owned. Then the baseline goes in: the Eight switched on for everyone, the Five Pages signed,

AI given an owner. Two pillars, one phase, because you can't secure a backbone that's still broken.

Scale and Grow. The marketing switched on. The Google listing, the website made to ring, the reviews engine, the CRM live, the first automations running, the Six Numbers on the dashboard. Last, because growth sits on the backbone, and the backbone isn't ready until it's fixed and the baseline's in.

Assess, Fix and Secure, Scale and Grow. Ninety days, start to finish, when it's done properly. Chapter 15 is what each one looks like week by week.

Four pillars. Three phases.

What gets owned, and the order the work happens in.

	Technology & IT	Cyber security	Digital marketing	Automation
01 / Assess Know what you have.				
02 / Fix & Secure Get the backbone right.				
03 / Scale & Grow Switch on growth.				

Circles show the focus of each phase.

Automation starts once there is a working system to automate.

WHY THE ORDER CAN'T CHANGE

Every firm that's rung me about marketing first has ended up doing the backbone first anyway. Because the ad lands on a slow site, the form goes to a dead inbox, the CRM's under a freelancer's login, and the AI assistant can't be switched on until someone's decided what it's allowed to say about clients.

Growth sits on the backbone. The backbone has to be fixed and locked first. That's the order, and the firms that skip it pay an agency to pour water into a bucket with a hole in it.

Automation's the same. It's the fourth pillar but it doesn't get its own phase, because you don't automate a mess. It lands inside Scale and Grow, once there's a system with real data running through it.

That's the shape. Four pillars, three phases, one owner.

Part three is the three ways to get there.

PART THREE

Three ways to fix it

CHAPTER 11

Three ways to fix it

You've seen what you've got. You've seen why it's leaking faster than it used to. You've seen the one idea that fixes it, and the shape of the fix.

The question now is who does it.

There are three answers. The way you're probably doing it now, with the vendors you've got. A newer way, where we show you our blueprint and you follow it with your own tools and your own people. And the way I think is best, where we do it, on our platform, with our people. The next three chapters lay them out side by side, with where each one falls down, including mine, because I'd rather you picked the right one than the one I make the most money on.

Whichever one you pick, do the Backbone Check first. The five questions at the end of chapter 1, or online at cxitservices.com.au/it-check, where you'll get a score and a plain-English read on what it means. Five minutes, no login, no sales call. If you're a reader of this book, your result's saved in your portal and I'll see it too. Not to chase you. So that if you ever do ring, I've done my homework.

Here they are.

CHAPTER 12

Do it yourself. The way you're probably doing it now

WHAT IT IS

Three vendors. An IT provider on tickets. A marketing agency on a retainer, or a web guy you haven't spoken to since the site went up. Someone who set up the CRM once. Whatever marketing you've tried, leaking out the holes from chapter 2. And you in the middle, refereeing.

When something's wrong, you Google it. When something's really wrong, you buy a course, or a plan, or a tool someone on LinkedIn swore by, and see what sticks. Mostly you put up with it, because the alternative's a project and nobody's got time for a project.

You've just read this book, so you could do it better than you have been. Hand chapter 3's checklist to the IT provider and say "show me". Hand them the Eight and the thirteen one percenters from chapter 4 and say "show me these". Run the Brochure Test on the web guy. Fill in the Five Pages. Put the Six Numbers in a spreadsheet and look at them on the first of the month.

And if you want to see what the outside world sees before you start, run the Firm Snapshot. You give us the firm's domain name. Nothing else. No logins, no access, no agent on a machine. We look at your firm the way an attacker and a prospect would, from out-

side. The security half: what's exposed, whether your email can be spoofed, whether the three email records are set, where you'd sit against Level 1 on the things we can see. The growth half: how the website performs on a phone, what the Google listing looks like, how many reviews and how recent, whether a search engine or an AI assistant can tell what you do. One report, both halves, scored, with the top five things to fix. It's a small paid product, because free things get ignored and the report takes real work. Details on the reader portal. Between that and the Backbone Check, you've done the Assess phase for the price of a coffee.

Plenty of partners will. It's better than nothing. Some firms do it well.

THE CHECKLISTS, COLLECTED

Everything in part one that you can hand to someone, in one place.

The Backbone Check (chapter 1). Five questions. Who owns the domain, when was the backup last restored, who wipes the lost laptop, who has admin rights, where are the passwords.

The Pointing Test (chapter 2). Five more. Who owns the domain, the tenant, the website login, the phone numbers, the CRM.

The Clean Switch (chapter 3). Thirteen things a provider should do when they take you on, and that you can make your current one do now.

The Monday Morning Eight (chapter 4). The Essential Eight as what 9am on a Monday looks like.

The one percenters (chapter 4). Thirteen boring things that aren't on the Eight, and the words to say to your provider.

The Five Pages (chapter 4). Acceptable Use, Passwords and MFA, Incident Response, Devices and Working Away, AI Use. One page each.

The Brochure Test (chapter 6). Six things to check on your own website from your phone.

The Six Numbers (chapter 7). What a partner looks at once a month instead of a marketing report.

All of them are in the reader portal as downloads, so you don't have to retype them.

WHO IT'S FOR

A firm with a practice manager who has the time and the authority, and vendors who are willing to be shown up a bit. It works. I've seen it done, and some of the firms that did it ended up being clients years later, in better shape than most.

WHAT IT COSTS

Whatever you're paying the three vendors now, which is usually more than one partner would charge. Plus the hours. The practice manager's, chasing. Yours, refereeing. And the ones nobody counts, which is every staff member's fifteen minutes a day.

WHERE IT FALLS DOWN

Nobody owns all of it. You can fix that for ninety days with a checklist and a stern meeting. Then someone leaves, or the agency changes, or the IT guy sells up, and it drifts straight back. The vendors are still three people who've never met, and you're still the only one who can see all three.

The old way isn't a plan. It's what happens when there isn't one.

And it's getting harder, not easier, for the five reasons in chapter 8. More tools, more places, more people asking you to prove things, and AI switched on across the lot. A practice manager with a checklist could hold the line in 2019. In 2026 she's holding it against a tide.

CHAPTER 13

Done with you. Own Your Technology

We call it Own Your Technology. The book says nobody does. This is where you start to.

WHAT IT IS

This book says what should be there. The course shows how to do it.

It's the same system, Assess, Fix and Secure, Scale and Grow, as a set of short videos of me actually doing the thing. One module per chapter of this book. Ten to twenty minutes each. Not theory. Screen recordings of the real work, on a real firm's setup, with the mistakes left in.

What's in it:

1. The Backbone Check, done properly, with the portal
2. The Pointing Test. Finding out who really owns your domain, tenant, phones, website and CRM, and getting them back
3. The Clean Switch. Moving providers without the week. The letter, the handover, the thirteen things
4. Devices. Enrolling them, encrypting them, patching them, taking admin rights away without a riot
5. Identity. Multi-factor on everything, the password manager, and the rules that stop the partner exception
6. Email. The three records, the filtering, and the quarantine rule
7. Backups. Setting them up, making them undeletable, and restoring something to prove it
8. The Five Pages. Each policy template filled in on screen for a real firm
9. AI. Finding what's already running in your tenant, writing the AI Use page, picking an owner
10. The Google listing and the reviews engine. Built, switched on, running itself
11. The website that rings. Speed, tap-to-call, booking, the AI assistant, and where the form actually goes
12. The CRM and the first two automations. Missed-call text-back and new client onboarding

Plus every template and checklist in this book, ready to fill in. The Five Pages as documents. The Clean Switch as a project plan. The Six Numbers as a dashboard.

Plus a community. You ask the question under the module it belongs to. I do a pass every week. An AI assistant that's read this book and every module answers the how-do-I questions in between.

Plus a live hour with me once a month. Bring the firm's problem. We work through it on screen.

Plus the growth tools from chapter 7, running on our platform for your firm. The AI assistant on your website, the reviews system, the CRM, the missed-call text-back. The same ones we run on ourselves. Switched on for you, with the course showing you how to use them.

WHAT IT ISN'T

It isn't the platform. You don't get the CX365 portal, the Beacon in the cabinet, the backups we run, the monitoring, the helpdesk, or the people. You run the blueprint on your own tools, with your own IT provider or your own in-house person doing the clicks, and you're the farmer. That's the point of it. It's also the limit of it.

WHO IT'S FOR

Firms under ten people, where a fully managed plan would be overkill and I'd be wasting your money. If you'd rather we owned the backbone underneath while you do the rest, there's a small bundle for that called CX365 Core, in the next chapter. Firms with an in-house IT person who needs the method and the toolkit behind them. And firms that aren't ready to change providers but have had enough of the limp, and want to run the system with someone in the room.

WHAT IT COSTS

A monthly membership that's less than an hour of a partner's time. Cancel whenever. Details on the reader portal.

WHERE IT FALLS DOWN

Someone at your firm still has to do it. The course makes it possible. It doesn't make it happen.

And there's a ceiling. Once a firm passes about ten people, the hours it takes to run this properly stop making sense for a practice manager to carry. At that point you've learned enough to know exactly what to ask the next provider for, which is most of the value.

The firms that outgrow the course are the ones I'd most like to talk to.

CHAPTER 14

Done for you. The best way

WHAT IT IS

Everything in this book, done by us. All four pillars, one owner, on the platform from chapter 9, with the 90 days in the next chapter.

The difference between this and the course is the platform and the people. You get the CX365 portal, the Beacon, the backups, the monitoring, the helpdesk, and a team whose whole job it is. The course shows you the blueprint. This is the blueprint, built.

In practice it means a managed plan with CX IT Services. We've got three, named for the Essential Eight levels they put you on, so the cyber baseline isn't something you tick, it's built into whichever one you're on. Ignite is Level 1. Secure is Level 2. Fortress is Level 3. Which one fits is set by what kind of firm you are, how many sites you have and what you handle, and we'll tell you before you've spoken to anyone.

Support that answers. The security baseline, switched on. The Five Pages, signed. Phones and internet, if you want them, under the same roof. The Google listing, the website made to ring, the reviews engine, the CRM, the first automations, the Six Numbers on the dashboard. The monthly report a partner reads. The quarterly review against the roadmap. Onsite visits that scale with your headcount.

One invoice. One number to ring. One name that owns the lot.

WHAT THE EXTRA BUYS

It costs more than the course and it costs more than muddling through, so I'll tell you what the extra actually buys.

First, a bit of perspective. If you've read this far, you've seen what's actually involved. The thirteen things in the Clean Switch. The Eight, and the forty-odd settings underneath them. The thirteen one percenters. The Five Pages. The ten things wrong with the website. The seven things that switch the marketing on. The Six Numbers. The first two automations. And all of it checked, every week, by someone who knows what they're looking at.

That's not a Saturday. That's a job. Several jobs, honestly, which is why most firms have three vendors and a gap. When you look at the number on the pricing page, that's what's behind it. Not a help-desk. The whole of part one, done, and kept done.

This is usually the point where it clicks for a partner, and I'll say it plainly in case it hasn't yet. We're not keeping the lights on. We're putting a system into your firm, the one you've just read, and running it with you, every week, for as long as you're with us. The lights staying on is a side effect.

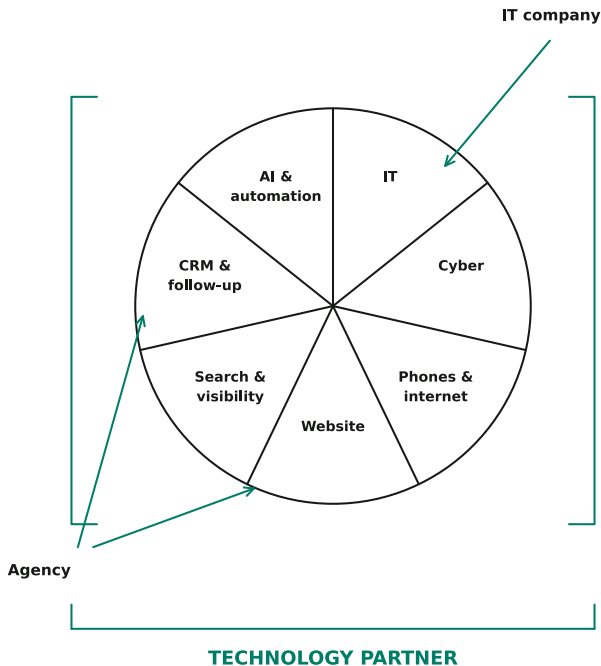
THE SLICE AND THE PIE

When a partner puts our number next to an IT company's quote, we look dear. When they put it next to the agency's retainer, we look dear again. Here's why that's the wrong comparison.

	Traditional IT company	Digital agency	Technology partner
IT support	Yes, measured on tickets	No	Yes, measured on fewer tickets
Cyber baseline	An add-on, if you ask	No	Built in, can't be declined
Phones and internet	Sometimes, separate bill	No	Yes, one bill, one number to ring
Website and hosting	No	Built once, then gone	Owned, hosted, watched monthly
Google listing and reviews	No	Sometimes	Yes, running on a system
Search and AI visibility	No	Yes, on a retainer	Yes, as part of the work
CRM and follow-up	No	Sometimes, under their login	Yes, under yours
Automation and the AI assistant	No	No	Yes
AI with an owner	No	No	Yes
Owens the joins between all of it	No	No	Yes
Measured on	Tickets closed	Traffic and green arrows	Whether the firm grows

The slice and the pie

Each vendor sells a piece. A technology partner owns the joins.



Seven slices. One partner accountable for the whole.

Each of them sells you a slice. Good slices, often. But to get the whole pie you'd be buying from three or four of them, paying three or four invoices, and still owning the joins yourself. Which is the pointing problem, with a bigger bill.

Put the invoices side by side and we're usually more expensive than any one of them, and cheaper than the lot of them. And the lot of them still doesn't give you one owner. That's not a slice. That's the platform, and it's why we cost what we cost.

And it's not a one-time job. Nothing in part one is a thing you do once and tick off. The patches land every night. The backups get checked every morning. The leavers get offboarded the day they leave. The reviews get asked for every time a matter closes. The Six Numbers get looked at on the first of every month. It's the gym from chapter 1. You don't get fit and stop. It's a way of life for the firm, and what you're paying for is someone who turns up to it every week so you don't have to.

It buys your time back. Not the practice manager's. Yours.

There's an old line about the difference between working in your business and working on it. Every hour a partner spends on a laptop that won't boot, a provider who won't call back, or a website nobody's touched since the agency left, is an hour working in it. Doing the job the firm was built to do for you.

I know because I did it to my own company.

For years I was the helpdesk. I was the onsite bloke. I was the one who built the thing and the one who got the call when it broke. CX ran on me, and it ran about as well as a firm runs on its managing partner's spare time.

Then I moved the helpdesk to a team whose whole job is answering the phone. I moved the onsite work to a field crew. I built the platform so nobody had to ring me to find out what was going on. Instead im now working on the business and its processes and focusing on growth - because the technology part is managed by CX365.

Its given me the time even write this book about it, and its how i see technology in the future.

That's the shift. Done for you isn't a bigger invoice for the same thing. It's technology off your desk and onto someone's whose whole job it is, so the hours go back where they belong. Clients. Staff. The next five years. A Friday afternoon.

WHO IT'S FOR

Firms of ten or more, with no in-house IT, who want the whole thing to stop being their problem. Which, if I'm honest, is most of the firms I talk to.

And under ten, there's a version of this too. We call it CX365 Core. It's the backbone done for you: internet, phones, Microsoft, patching and protection on the devices, the website hosted, for one site and up to ten people. Without the helpdesk and without the full cyber tiers, because at that size you don't need them yet and I'm not going to charge you for them. Pair Core with the course and you've got the backbone owned by us and the rest done with you. It's not on the pricing page, it's a conversation. And when you hit ten, it hands straight across to the managed plan, because that's exactly the size where a firm stops being able to self-manage.

Also firms with an in-house IT person who's drowning. That's a co-managed arrangement: your person does the day-to-day and the firm-specific stuff, we provide the platform, the baseline, the escalation, the after-hours and the roadmap. They get a better toolkit and a team behind them. The one thing we won't do is split ownership of the backbone. Someone has to own all of it, and we agree up front who.

WHAT IT COSTS

Per user, per month, and it's on our website. I'm not going to put numbers in a book, because they'll be out of date before the ink's dry and because I'd rather you looked at the page with your own headcount in it. What I'll say is that every firm your size pays the same rate, there's no quote, and there's no three-year contract on day one. Chapter 16 has the bit about how it scales as you grow.

WHERE IT FALLS DOWN

If you're under ten people, the full managed plan is too much, and I'll say so. The answer there is Core plus the course, not a plan built

for thirty. I'd rather lose the sale than sell you something you don't need.

And if you want to keep your current marketing agency, that's fine, as long as the plumbing under them is ours: the domain, the DNS, the hosting, the form routing, the CRM. The agency does the creative. We make sure it lands. Most of the pointing problem goes away the moment one party owns the joins, and a good agency will be glad of it.

The next chapter is what the first 90 days look like when we do it.

CHAPTER 15

The first 90 days

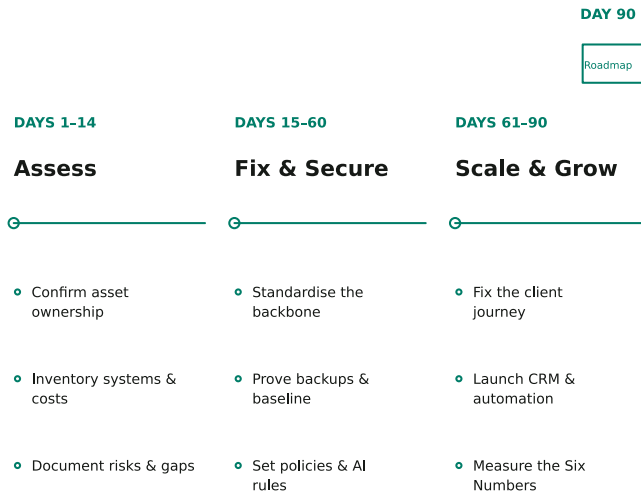
The thing partners fear most about changing providers isn't the cost. It's the week. The week where nothing works, the email bounces, the printer vanishes, the practice management system logs everyone out and there's a client at the front desk with a laptop that won't connect.

So most firms stay. Not because the provider's good. Because the switch feels worse.

Here's the switch, phase by phase, the way we actually do it. The whole point is that your staff shouldn't notice the week happened.

The 90-day Reset

Three phases. A working baseline. One page for the year ahead.



THE ROADMAP

Where you are. What comes next. What it costs.

The sequence matters: assess, fix and secure, then scale and grow.

ASSESS: DAYS 1 TO 14

The first fortnight is paperwork, and it's the most important fortnight of the ninety days, because it's when we answer the Pointing Test for you.

You tell your current provider you're leaving. That's the one thing we need you to do, and we'll give you the words. From there, we deal with them directly. We've built an onboarding and offboarding system specifically for this, because we've done it enough times to know exactly what to ask for and in what order: the admin

credentials, the documentation, the licence details, the backup access, the domain, the phone numbers, the lot. Most providers are professional about it, because they've been on the other side. If there's no documentation, and there often isn't, we build it.

We run the Snapshot, if you haven't already. We open the cabinet nobody opens. We list every piece of software the firm pays for, and what it costs, and who uses it. That list is usually the first saving and the first shock.

By day 14 we know, and you know, in writing:

- Who owns the domain, and it's now in the firm's name if it wasn't
- Who holds the Microsoft tenant, and the firm now holds the top-level account, with us as a delegated partner, not the owner
- Every user account, and which ones belong to people who left in 2023
- Where the files live and whether the backup has ever been tested
- The phone numbers and whose name the account is in
- Every subscription, its cost and its owner
- What the outside world sees, on security and on growth

All of it in the portal. Your portal. From day one.

FIX AND SECURE: DAYS 15 TO 60

Weeks three and four are the backbone.

Every laptop and desktop comes under management. We can see it, patch it, protect it, and wipe it from a phone if it's left in a cab. A small agent installed quietly over a couple of days. Nobody's machine gets wiped. Nobody loses a bookmark.

The helpdesk goes live. Your staff get one number and one email. When they call, a person answers.

The network gets documented and, if it's mismatched or tired, replaced with our standard kit. The Beacon goes in. The internet gets

sized for the firm now. The phones come across, if you've chosen that, and the numbers go into the firm's name.

Backups get set up properly, and then we restore something. A real file, from a real backup, to prove it works. You'll get a screenshot. Keep it.

By day 30 your old provider's gone, your licences are consolidated, your gear is standard, your backups are proven, and you've had the first invoice. One invoice. Four lines. Nothing else.

Weeks five to eight are the baseline.

Most of it came with the platform. Multi-factor, device protection, web filtering, backups and the password manager were switched on in the first month. The Secure half isn't installing them. It's proving they're on, for everyone, with no exceptions, and then dealing with the things that are about people rather than software.

The Monday Morning Eight, checked off one at a time, with evidence in the portal. Admin rights removed from everyone, partners included, with a quiet week of "it still works, doesn't it" afterwards.

The Five Pages. We sit down with you for an hour, fill in the firm's specifics, and they go in the portal for staff to acknowledge. The AI Use page gets an owner. The portal shows which AI tools are already running on the firm's devices, and the owner decides what stays.

The insurer's questionnaire, filled in with you, honestly, with the evidence to back every yes.

By day 60 the firm's on the baseline, the paperwork's honest, and AI has an owner.

SCALE AND GROW: DAYS 61 TO 90

Now, finally, the front door.

The Google listing gets completed properly. Every service, the right category, real photos, and reviews flowing in and replied to.

The website gets fixed, not rebuilt. Fast on a phone. Tap-to-call. A booking link. The chat switched on, answered by the AI assistant that knows your rules from the Five Pages. The form routed to a human who sees it in minutes.

The reviews engine goes live. When a matter closes or a return is lodged, the client gets a short message with a link.

The CRM goes live, under the firm's login, with every enquiry from every channel landing in it.

The first two or three automations. Missed-call text-back on day one of this phase, because it's the highest return. Then new client onboarding, or appointment reminders, or whichever one saves the most hours at your firm.

The Six Numbers appear on the dashboard, next to the ticket count and the backup status.

And if ads make sense for your firm, they start now, because for the first time there's a page that converts and a number someone can read.

DAY 90: THE ROADMAP

On day 90 you get one page.

Four columns, one per pillar. Technology and IT. Cyber. Marketing. Automation. Down each column: where you are now, honestly, including the things we found that aren't urgent and need a date. What we'd do next, in order, two or three things per column with a quarter against each. And what each costs, and what it saves or earns.

A partner can read it in ten minutes and make decisions for the year.

The Roadmap one-pager

A page a partner can read in ten minutes and use all year.

YOUR FIRM / TECHNOLOGY ROADMAP			
Next 12 months • Prepared at day 90			
Technology & IT	Cyber	Marketing	Automation
WHERE WE ARE	WHERE WE ARE	WHERE WE ARE	WHERE WE ARE
WHAT COMES NEXT	WHAT COMES NEXT	WHAT COMES NEXT	WHAT COMES NEXT
COST / RETURN	COST / RETURN	COST / RETURN	COST / RETURN

Four columns. Three decisions. One accountable owner.

Here’s the shape of one, for a thirty-person accounting practice. Not a real firm’s numbers. The shape of a typical one.

Technology and IT. Next quarter: replace the eleven laptops older than four years, staged, three a month. Quarter after: the Wi-Fi in the boardroom. Later: the practice management upgrade, scheduled for the quiet week after lodgement season.

Cyber. Now: Level 1, done. Next quarter: staff awareness training, because the clock-drift story made everyone laugh and nobody’s

done the course. Mid-year: move to Level 2, because the firm handles SMSF audits and the insurer asked.

Marketing. Now: the Six Numbers are live and enquiries are up. Next quarter: a content program answering the forty questions prospects actually ask, so the AI search engines start naming the firm. Mid-year: a decision on ads, based on what two quarters showed.

Automation. Now: onboarding and missed-call text-back running. Next quarter: the monthly client update email. Mid-year: the new-starter automation, because the firm's hiring.

THEN YOU DECIDE

Up to day 90 you've been month to month. If at any point in those 90 days you decide it isn't working, you walk. No exit fee, no argument. Your documentation, your credentials and your data go with you in a clean handover, the same way we'd want to receive them. I can offer that because almost nobody takes it, and the few who have, I'd rather know early.

At day 90, with the roadmap in your hand, you pick a term, or stay monthly. That's a conversation for then, not for a book.

AFTER THE 90

The rhythm settles.

Every month, the report and the Six Numbers. Every quarter, a review against the roadmap: what got done, what moved, what we learned. Not a sales meeting. A working session with the person who knows your firm.

Onsite visits on the schedule your headcount sets. The helpdesk answering. The patches landing at 2am. The backups checked every morning. The one percenters, every day, that you never think about, which is the whole point.

And at month twelve, a new roadmap. A bit further along. A bit more ambitious. Because a firm whose backbone's been right for a year can do things a firm with a limp can't.

THE HONEST VERSION OF THE PROMISE

I've been promising you more clients and less chaos since the first page. Here's what that means by day 90 and what it means by day 365.

By day 90 the chaos is gone. That part I'll stand behind for every firm. The backbone's fixed, the baseline's in, one name owns the lot, and the stuff that used to eat your Friday afternoons doesn't anymore.

The clients take longer. The marketing's switched on at day 90 and measured from then. For most firms the Six Numbers start moving within the first quarter after that, and by month twelve the firm's getting enquiries it never used to get, from channels it never used to have. But I won't promise you a number of clients by a date, because anyone who does is guessing, and you'll know it.

What I'll promise is that for the first time, growth will be something you can see, measure and steer. For most firms, it's the first time technology has ever been pointed at the front of the business instead of the back.

Growth. How it scales with you

A firm that's done the Reset grows. That's the point of it. So the last thing to cover is what happens to the technology, and to us, when it does.

USERS

The plan's per user, per month, and every user is a user. We tried pricing part-timers differently once, years ago. It was a nightmare to administer and nobody was happier, so now it's one rate and it scales with your headcount, up and down, month to month.

A new starter is a form. By the time they arrive they've got a login, a laptop, a phone extension and the right software, and their first morning isn't spent waiting for IT. A leaver is the same form in reverse, and their access is gone the same afternoon. At twenty staff that's a convenience. At eighty it's the difference between a firm that can hire and one that can't.

DEVICES

Every device is under management from the day it's unboxed to the day it's wiped and retired. Laptops get replaced on a cycle, not when they die. The roadmap tells you which ones are due next quarter, so there's never a surprise bill for eleven at once.

The network gear is yours outright from day one, and the monthly site fee funds its replacement over time. When it's five years old and tired it gets swapped, and you don't get a capital bill.

SITES

A second office is a Beacon, a connection, a Wi-Fi and a phone extension range. We've done it enough times that it's a checklist, not a project. Melbourne, Sydney, Brisbane, Perth, the regions, across the Tasman. The platform's in the cloud, the helpdesk is a phone call, and onsite runs through a field partner network so the Brisbane office gets the same as the Melbourne one.

The only thing distance changes is that it might not personally be us plugging in your switch. The person who is will be working from our documentation and our standard.

RESOURCES

Here's something business owners forget, and it's not their fault, because the industry's never said it out loud.

Your IT provider is an employee. You've just outsourced them.

That's what the monthly fee is. Two things. The labour to look after the business, which is a salary, split across the firms the provider looks after. And the licensing and services for the whole firm: a Microsoft licence for every user, backups for every mailbox and every file, the security tools on every device, the monitoring, the filtering, the phones, the internet. Labour and kit, for everyone. Same as putting an IT person on your payroll and then buying them everything the firm runs on, except this one comes with the tools included and doesn't take annual leave.

So when a partner asks for the fee to come down, what they're actually asking is for that employee to do the same hours for less pay, or the same pay for fewer hours, or for the firm to run on fewer licences than it's got people. Nobody says it like that, because it sounds unreasonable when you do. It is unreasonable. You can't

get a full-time result out of a part-time salary, and you can't run the Eight on half the tools.

Plenty of IT companies drop their price anyway, to win the deal. I've watched it happen and I've watched what comes next. The provider can't afford the hours, so the hours quietly shrink. The patching slips. The leaver doesn't get offboarded until Friday. The backup nobody's checking fails. Six months later the firm's got the limp back, the provider's losing money on the account, and each of them thinks the other one's the problem. The discount didn't save anyone anything. It moved the cost to the day something broke.

That's why our rate is what it is. It's the salary it takes to do the job properly for a firm your size. And it's why the rate doesn't fall as you grow, which is the next bit, and the bit that gets a reaction.

Here's where we part ways with most of the industry.

Most industries work on volume. More seats, lower rate. It feels natural, so firms ask for it.

But think about what a bigger firm actually needs. More devices to manage. More users to onboard and offboard. More places for something to go wrong. More compliance exposure. More onsite time. A sixty-person firm doesn't need less of us per person than a twenty-person firm. It needs more.

So the per-user rate doesn't fall as you grow. What changes is what's included.

Under thirty staff, onsite is there when you need it, at an hourly rate, and most of what you need is done remotely anyway.

At thirty, you get a scheduled onsite visit every month. Someone walks the floor, checks the cabinet, talks to the staff who never log a ticket but have been living with something for six months.

At sixty, it's fortnightly.

At ninety, it's weekly.

Past a hundred and twenty, you've got a named engineer who's in your office twice a week, knows your systems better than some of your staff, and knows where the good coffee is.

The rate stays. The resource grows with you. That's not us being difficult. That's us being honest about what it takes to look after a firm properly at each size.

GROWTH, THE OTHER KIND

The marketing scales too, and it scales differently.

The Google listing, the reviews engine, the CRM, the missed-call text-back, the AI assistant, the Six Numbers, these are in the plan. They sit on the platform, so they cost us little extra and we'd rather you had them.

A full website rebuild, an ongoing ad budget, a proper search and content program, video. Those are real work with real hours, and every firm's different, so they're quoted, and they show up on the roadmap as a choice with a number against it. Never a surprise.

What changes as you grow is ambition. At twenty staff the goal is a website that rings and reviews that flow. At sixty it's a content program that makes the AI assistants name you first in three cities. At a hundred it's a pipeline a partner can forecast from. Same platform, same owner, same Six Numbers. Bigger numbers.

AND THE AI

The last thing that scales is the thing most firms are nervous about.

AI in your firm is going to grow whether anyone owns it or not. More tools, more staff using them, more data going in, more agents running in the background. The firms that handle it well will be the ones where one name owns it, the AI Use page is current, the portal shows what's running, and the next tool someone switches on gets noticed in a week, not a year.

That's not a feature. It's the pointing problem, solved, for the thing that's about to matter most.

Nobody owns your technology. Including the AI. Someone should.

Questions partners ask

The ones I get most. Straight answers.

WE ALREADY HAVE AN IT PROVIDER AND THEY'RE FINE. WHY WOULD WE CHANGE?

Maybe you shouldn't. "Fine" is a legitimate place to be.

But "fine" is also where most firms are the day before something isn't. Fine usually means nothing's broken that you know about. It doesn't mean anyone's looked under the waterline. Your IT guy isn't going to ring you to say he's behind on patching and never tested the backup. The web guy isn't going to mention the form's been going to a dead inbox since March. Nobody reports their own gaps. It's not dishonesty. It's that nobody asked, and nobody's measuring. That's the false sense of security most firms are sitting in, and it feels exactly like fine.

So do the Backbone Check. If you got five clean answers, stay, and I mean that. If you got "umm" on two, "fine" is doing a lot of work in that sentence. And ask the chapter 2 question: has your IT provider ever been asked about leads? If the answer's no, you're paying for a quarter of the job.

What you're actually after isn't a new provider. It's accountability and transparency. Someone who shows you the inside, on a screen, every month, including the bits that aren't going well. If your

current provider will do that, keep them. If they won't, that's your answer.

HOW DOES SWITCHING WORK, AND WILL WE LOSE A DAY?

Chapter 15. We handle the handover with your old provider, your staff get one new number, and the swap happens in the background. The week where nothing works is the thing partners fear. We've done this enough times that it doesn't happen.

WHO ACTUALLY ANSWERS THE PHONE?

A person. An Australian-based helpdesk with overflow so the phone doesn't ring out at 8:30 on a Monday, who can see your firm on the screen when they pick up. Business hours is standard, extended and 24/7 are options.

WE'RE IN PERTH. OR REGIONAL VICTORIA. OR AUCKLAND. DOES THAT WORK?

Yes. Chapter 16. The platform's in the cloud, the helpdesk is a phone call, and onsite runs through partners across Australia and New Zealand.

WHAT IS THE ESSENTIAL EIGHT, AND DO WE LEGALLY HAVE TO DO IT?

Chapter 4. The government's list of the eight things that stop most attacks, with the forty-odd settings underneath them. Not the law for a private firm, but your insurer, your bigger clients and any tender will ask. Level 1 is the pass mark.

You'll also hear about SMB1001:2026. It's a cyber security standard written for small and medium businesses, with tiers from Bronze upwards and a certificate at the end you can hand to an insurer or a client. Same work, same goal, different badge. If you've done the Eight at Level 1 you'll clear the lower tiers comfortably, and we can take you through the certification if you want the piece of paper. Some firms do, because a certificate answers the questionnaire before it's asked.

OUR CYBER INSURANCE RENEWAL IS ASKING QUESTIONS WE CAN'T ANSWER. WHAT NOW?

Don't guess. A wrong answer is what gets a claim denied. Answer honestly, and where it's "not yet", give a date. After Fix and Secure, the honest answer to nearly all of it is yes, with evidence. We'll fill the form in with you.

WHAT HAPPENS ON DAY ONE IF WE GET BREACHED?

Chapter 4, last section. Contain in the first hour, understand in the first four, tell the insurer and work out the notification obligations on day one. The point of the baseline isn't that nothing ever happens. It's that when it does, it's small and you know what to do.

DO YOU WORK WITH LEAP, FYI DOCS, APS, BGL, HANDISOFT, MYOB?

Yes. Those are the systems we've spent 26 years inside. This is a professional services technology company. It's the whole point.

CAN WE KEEP OUR OWN MARKETING AGENCY?

Yes, as long as the plumbing under them is ours: the domain, the DNS, the hosting, the form routing, the CRM. The agency does the creative. We make sure it lands, and we make sure it's secure. An agency with a login to your website and your DNS is one more set of credentials nobody's watching, and we've seen that end badly. Under us, they get what they need to do their job and nothing they don't.

WE HAVE SOMEONE DOING IT IN-HOUSE. CAN YOU WORK ALONGSIDE THEM?

Yes. Co-managed. Your person does the day-to-day, we provide the platform, the floor, the escalation, the after-hours and the roadmap. The one thing we won't do is split ownership of the backbone.

WHO OWNS OUR DATA, OUR DOMAIN AND OUR MICROSOFT TENANT?

You do. All of it. The first fortnight makes sure of it. If you ever leave, it goes with you. I've seen firms held hostage by a provider who owned the domain. It won't be us.

CAN STAFF USE CHATGPT AND COPILOT?

Yes, with rules. The AI Use page says which tools are approved and what can't go in them. The portal shows what's actually being used. Banning it is the wrong answer. Not knowing is worse.

WE'RE UNDER TEN STAFF. IS THERE ANYTHING FOR US?

The course, chapter 13, and CX365 Core, chapter 14. Under about ten people a firm doesn't need a fully managed plan, and I'd be wasting your money selling you one. Core is the backbone done for you. The course is the rest, done with you.

WHAT IF IT DOESN'T WORK OUT?

You walk, in the first 90 days, no exit fee, with a clean handover of everything. I can offer that because almost nobody takes it, and because if a firm isn't happy I'd rather know early. We're all on the same team or we're not.

One last thing

I started CX because I thought firms like yours deserved technology that didn't need thinking about, from people who thought about it so you didn't have to. The one percenters. Eight years on, that's still the whole idea. It just turned out the one percenters included the phones, and the website, and the marketing, and the AI, and a book.

Nobody owns your technology. We'd like to.

More clients. Less chaos. Ninety days.

Peter Nelson

Director, CX IT Services

cxitservices.com.au · 1300 477 814

AT THE BACK

The Backbone Check. Five questions, five minutes, a score. cxitservices.com.au/it-check

The Firm Snapshot. Your firm from the outside, security and growth, one report. Domain name only. Details on the reader portal.

Own Your Technology. The do-it-with-you version. Twelve modules of me doing the work on screen, every template and checklist in this book, the Five Pages ready to fill in, a monthly live hour, a

community, and the growth tools running for your own firm. Details on the reader portal.

Done for you. cxitservices.com.au

Every checklist in this book, as a download, on the reader portal.

You have providers. But who owns the whole thing?

Your IT company keeps the computers running. Your agency looks after the website. Someone else set up the phones, the CRM and the automation.

Each owns a piece. You live with the gaps.

The slow laptop. The enquiry nobody followed up. The backup nobody tested. The AI tool nobody approved. Small problems that quietly cost your firm time, money and clients.

Peter Nelson shows you how to take back control of the whole picture: IT, cyber, phones, internet, website, search, ads and AI. With practical checks and a clear 90-day Reset, you will know what you have, what needs fixing and who is accountable.

Do it yourself. Do it with help. Or have it done for you.

More clients. Less chaos. One owner.



PETER NELSON | Director, CX IT Services

26 years in IT. A practical approach to technology for professional services firms.

cxitservices.com.au

