

GUIDE · IT AND SECURITY

Setting up IT for a firm that has never had any.

Nobody planned your IT. It accumulated — a router from the internet provider, a shared drive somebody set up, licences bought one at a time as people joined, and a server in the corner that a contractor built and nobody has logged into since. It works, mostly. This is what it costs you that it works mostly, and what six specific decisions would change.

No email required. Nothing gated. If you take all of it, hand it to your existing provider and never speak to us, the guide has done its job.

Contents

- 1 Why this is worth an afternoon of your attention
- 2 Working from anywhere, properly
- 3 The office network, and why large files punish a cheap one
- 4 Standardised internet access: faster and safer are the same job
- 5 Licences: the money most small firms leave on the table
- 6 Something watching, and a person reading it
- 7 Accounts, identity and the leaver problem
- 8 The order to do it in

1 Why this is worth an afternoon of your attention

The cost of unplanned IT is almost never a bill. It is a slow leak: the twenty minutes a file takes to open over the wrong connection, the afternoon lost when someone works from home and cannot reach the drive, the licence renewed for a person who left, the hour your most capable employee spends being the IT department instead of doing the job you hired them for.

None of those show up anywhere you would notice. Added together in a firm of ten, they are comfortably a day a week, and the day comes out of the people you can least afford to lose it from.

The other cost arrives all at once, and it is the one that closes firms: the ransomware that spreads because everyone is an administrator, the backup that turns out never to have been restored, the client questionnaire you cannot answer that stalls a contract you had already won.

Six decisions cover most of both. None of them are exotic and none require a full-time IT hire.

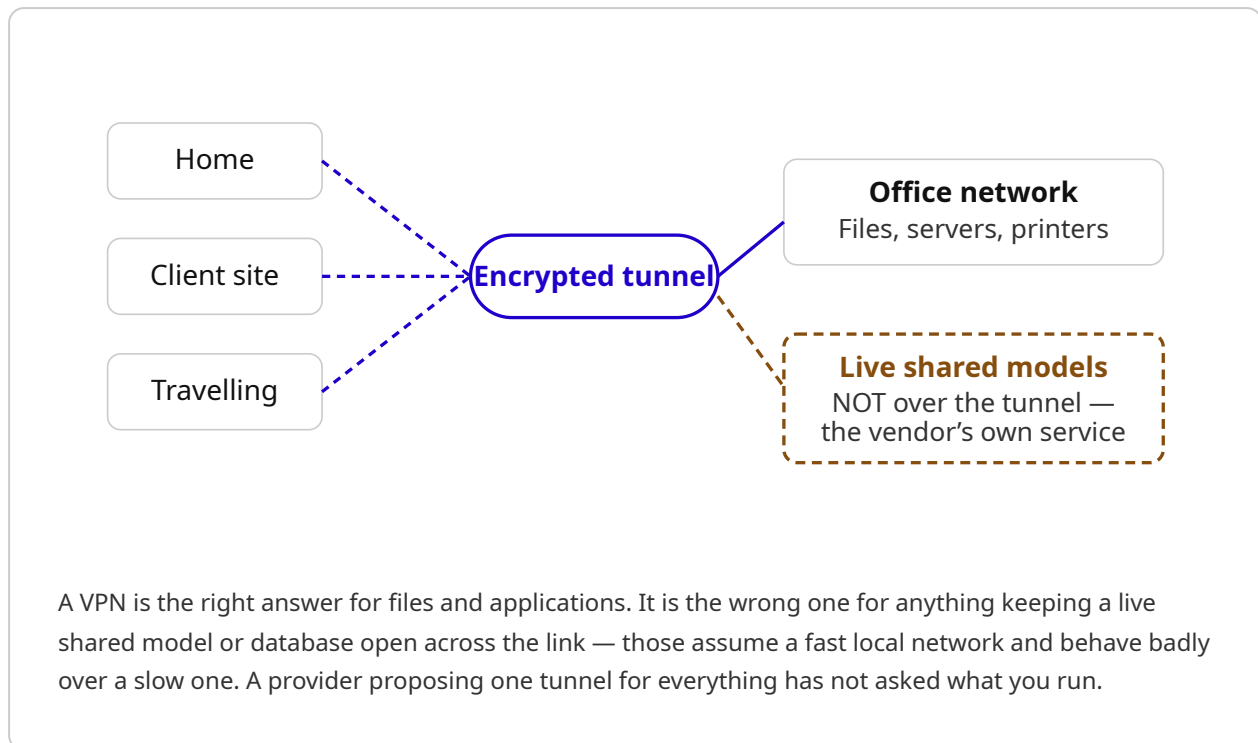
2 Working from anywhere, properly

What it costs you today. Someone is at a client site and cannot open the file they need, so the meeting ends with “I will send it over” and the decision waits a day. Someone works from home and emails themselves a copy to work on, which becomes the version nobody else has. Both are the same missing thing.

What to do. Remote access that does not depend on copying files around. In practice that is one of two shapes: everything the business works on lives in a cloud workspace and is reachable from anywhere by design, or a VPN connects a laptop back to the office network so the shared drive behaves the same from a kitchen table as from a desk.

Most firms end up with both — cloud for documents, VPN for the things that have to stay in the building. The decision worth taking deliberately is which category each system is in, because the answer drives the backup plan, the access list and the cost.

One caveat worth knowing before somebody sells you the wrong thing. A VPN is right for reaching files and applications. It is the wrong answer for software that keeps a live shared model or database open over the network — design and engineering tools in particular — because those were built assuming a fast local connection and behave badly across a slow one. That case needs the vendor's own collaboration service instead. A provider who proposes "VPN to the file server" for everything has not asked what you run.



The outcome: the same working day wherever it happens, and one copy of every file.

3 The office network, and why large files punish a cheap one

What it costs you today. If your work involves large files — drawings, models, video, scans, photography — the office network is a productivity tool, not plumbing. A 2 GB file over a saturated wireless connection is minutes of waiting, several times a day, per person. People respond by keeping local copies, and now you have a version problem as well as a speed problem.

What to do. Three unglamorous things, in this order:

- **Wire the heavy seats.** Anyone moving large files or driving a graphics-heavy application should be on a cable, not wifi. It is the single cheapest speed improvement available and it is usually a morning's work.
- **Business access points, not a provider's router.** A consumer router doing the job of an office network is the most common thing we find. Proper access points cover the space evenly, hand a laptop over cleanly as someone walks, and separate the staff network from the one you give visitors.
- **A separate network for guests and devices.** Visitors, phones, the printer and anything smart belong away from the machines holding client work. This is one setting on the right equipment and it limits how far a problem on any of them can travel.

Opening one large project file

Wired to the office server

 seconds

Business wifi, quiet office

 a wait

Shared consumer wifi, everyone working

 minutes, every time

Relative, not measured — the point is the ORDER, which holds for any firm whose work is drawings, models, video or scans. People respond to the bottom bar by keeping a local copy, so a slow network quietly becomes a version-control problem as well.

The outcome: large files open at the speed the disk can manage rather than the speed the wifi allows, and collaboration happens on one copy because working on one is no longer slower than keeping your own.

4 Standardised internet access: faster and safer are the same job

What it costs you today. A meaningful share of what your connection carries is advertising and tracking that nobody in the building wanted. It uses bandwidth you paid

for and it makes every page slower to load, which is a small tax collected many times a day.

Filtering at the network level — deciding which addresses the office is allowed to reach, once, for every device — removes most of it before it is ever requested. The same mechanism blocks known phishing and malware sites, which is why this is a security control and a performance improvement at the same time.

One office connection, one month

← filtering removes these two →



- Your actual work
- Advertising and tracking
- Known-bad destinations

Proportions illustrate the cited range (25–40% of traffic removed by blocking), not a measurement of any particular office. Filtering removes the two right-hand bands before they are ever requested, which is why the same control makes the connection faster and safer at once.

25–40%

Less network traffic with ads blocked — 25% on ordinary browsing, 40% where streaming video is involved. Simon Fraser University.

Source (<https://venturebeat.com/business/blocking-ads-can-cut-network-traffic-25-to-40-study-shows>)

25–34%

Reduction in data transferred, averaged across the major blockers, in a peer-reviewed measurement study.

Source (<https://arxiv.org/pdf/1705.03193>)

Both figures measure browser ad blocking on consumer web browsing. Network filtering in an office is the same mechanism against a different mix of traffic: if most of your bandwidth is project files, the share you recover is smaller. We quote the studies rather than a number of our own because we have not measured your network — that is what the review is for.

What to do. Point the office network at a filtering resolver, turn on the categories that matter — advertising, tracking, known malicious and phishing domains — and leave the rest alone. Resist the temptation to block categories on grounds of productivity: it generates arguments, people route around it, and it buys nothing.

The outcome: a connection that carries your work instead of somebody else's advertising, and one fewer way for a mistaken click to end badly.

5 Licences: the money most small firms leave on the table

What it costs you today. Specialist software is usually bought one seat at a time, as people join, on whichever plan was in front of whoever bought it. Nobody revisits it. So a firm of eight ends up paying for eight of everything, including tools that two people open once a month, and for at least one seat belonging to somebody who left.

What to do. Find out which of your tools support *floating* licences — a shared pool where a licence is checked out while someone is using it and returned when they close the application. Where a tool offers it, a pool sized to how many people actually work at once is usually smaller than your headcount, and the saving is immediate and permanent.

Not every vendor offers it, and the landscape changes: several have moved from network licensing to named users in recent years, and some of those offer a token or pay-as-you-go plan for occasional users instead. The work is an inventory — what you own, who actually opens it, and which model each vendor sells today — and it is usually an afternoon that pays for itself in the first month.

While you have the list open, tie each licence to a person in your account records. It is the only way the renewal for a leaver ever gets cancelled.

Bought per seat

Eight people, eight licences — including the two who open it once a month

Shared pool

A licence is checked out while it is open and returned when it is closed — so you buy for concurrent use, not for headcount.

Only some vendors offer a pool, and which ones changes — several have moved to named users, with a token or pay-as-you-go plan for occasional use instead. The work is an inventory: what you own, who actually opens it, and what each vendor sells today.

The outcome: you pay for concurrent use rather than headcount, and no renewal outlives the person it was bought for.

6 Something watching, and a person reading it

What it costs you today. Most damage to a small firm is not discovered by the firm. It is discovered by a customer, a bank, or the morning everything stops. The gap between something starting and somebody noticing is usually measured in weeks, and almost everything that makes an incident expensive happens inside that gap.

What to do. Collect the signals your systems already produce — sign-ins, laptops, servers, email and cloud accounts — into one place that can raise a flag. The tooling for the collecting is a SIEM; extending it past the network to the devices and accounts themselves is what the industry calls XDR. Both are worth knowing only because you will see them on a quote.

What nobody will tell you when they sell it. A new deployment is noisy for the first few weeks, and tuning that noise down is most of the work. Anyone promising a quiet console on day one is describing a product demo. The question to ask a provider is not what their

tool detects — it is who reads the alerts, how quickly, and what happens at two in the morning.

The outcome: somebody finds out the day something changes, instead of a customer telling you three weeks later.

7 Accounts, identity and the leaver problem

What it costs you today. Ask who still has access to something and most firms answer “probably somebody”. That is not carelessness. It is what happens when logins were created tool by tool over several years, because there is no single place to remove a person from.

What to do. Put one account per person at the centre — a company identity through your email and document provider — and connect everything that can connect to it. Four things follow, and none of them are possible without it:

- **Removing access in one place** when somebody leaves, rather than in twelve, from memory, on their last afternoon.
- **Two-step verification everywhere at once.** The cheapest control there is, usually free, and the first line of every client security questionnaire.
- **No shared logins.** A shared account for a licence portal or the bank is normal and understandable, and it is why nobody can say who did what — and why one person leaving means changing a password for everyone.
- **Ordinary users, not administrators.** If everyone can install anything, a bad click reaches everything. This is the setting most likely to annoy people if it is changed badly, so it is worth agreeing rather than imposing.

Encrypt the laptops while you are here. It is already built into the machines you own and usually just not switched on, and it is the difference between losing a laptop and telling your clients you lost their files.

The outcome: a ten-minute offboarding that actually works, and an honest answer when someone asks who can reach what.

8 The order to do it in

Not all six at once, and not in the order a vendor would like. Cost and risk both fall fastest in roughly this sequence:

1. **Find out what you have.** Every machine, service and account; what is exposed; who can reach what; and whether the backups restore. Everything below is guesswork without it, and it is usually a week.
2. **Restore a backup in front of somebody.** Not a report saying backups ran. An actual file, recovered, watched. This is the one that changes minds, and it is cheap.
3. **One account each, with two-step on.** Free or close to it, and everything else in access control depends on it.
4. **The network:** wire the heavy seats, put in real access points, turn on filtering. Fastest visible improvement, and the one people thank you for.
5. **The licence inventory.** Often pays for the steps above.
6. **Then monitoring.** Last, because watching an estate you have not tidied generates alerts about problems you already knew you had.

If you only ever do the first two, you will have removed most of the risk that actually closes small firms, and you will know enough to argue with anybody who quotes you for the rest.

Want to know where you stand before reading any further? The [five-question check](#) takes a minute and answers back immediately, and the [full questionnaire](#) covers everything in this guide.