



A GUIDE FROM THE KING OF CYBERSECURITY

WHERE TO START

Cyber security for small businesses, beginning with the only question that has to come first: what have you actually got?

Free. No sign-up. Print it and tick it

Sixteen things. Most people have five or six of them. Nobody has all sixteen, and the ones you do not have are the ones you can stop worrying about. Tick only what applies: a short list is a finished answer.

Filled in by whoever has day-to-day access to most of these things. Reviewed by whoever needs to know the result. They are often not the same person, and the form is built to travel between them: the notes on pages three and four explain every line, so the answers make sense to somebody who was not there when it was completed.

Business

Completed by

Reviewed by

Date

TICK WHAT YOU HAVE

WHO CAN GET TO IT — TICK ALL THAT APPLY

ME

STAFF SUPPLIER

EVERYONE HAS THESE

☐	A A business email address Who can get into it?	☐	☐	☐
☐	B Online banking Who can authorise a payment?	☐	☐	☐
☐	C A phone you use for work What is already signed in on it?	☐	☐	☐
☐	D At least one computer Is it still getting security updates?	☐	☐	☐
☐	E Files you could not lose Where is the second copy?	☐	☐	☐

MOST BUSINESSES HAVE THESE

☐	F A domain name Whose name is it registered in?	☐	☐	☐
☐	G A website Who can change what it says?	☐	☐	☐
☐	H Cloud storage What is shared by link outside the business?	☐	☐	☐
☐	I Social accounts Who knows the password?	☐	☐	☐
☐	J Accounting or payroll software Who can log in to it?	☐	☐	☐

ANYONE WITH STAFF HAS THESE

☐	K Staff accounts and logins How does someone lose access when they leave?	☐	☐	☐
☐	L Devices they own themselves Whose phones and laptops hold work data?	☐	☐	☐

SOME BUSINESSES HAVE THESE

☐	M Card payments or customer records Where is customer data stored?	☐	☐	☐
☐	N Suppliers with access to your systems Which outside companies can log in?	☐	☐	☐
☐	O Software you build or have built Who can change the code and release it?	☐	☐	☐
☐	P Insurance Does your policy cover a cyber incident?	☐	☐	☐

Every line is explained on pages three and four. Staff and supplier ticks carry on to page five.

WHAT EACH LINE MEANS

Me is you. **Staff** is anyone inside the business, including part-time and family. **Supplier** is anyone outside it who can log in. More than one is normal.

If in doubt, tick it: a line ticked in error costs a minute, and a line missed costs the point of the exercise.

A A business email address

Any address you use for work, including a free personal one. If mail for the business arrives there, it counts. Tick “supplier” as well if an IT provider set it up or could reset the password.

B Online banking

Business or personal, if the business’s money moves through it. Count everyone who can authorise a payment, including a bookkeeper or accountant with their own login.

C A phone you use for work

Yours or the company’s. If work email, messages or authentication codes reach it, it is in scope. The useful thing to picture is what is already signed in on it.

D At least one computer

Every machine used for work, including a home one. “Out of support” means the maker no longer issues security updates for it, which is different from it being slow.

E Files you could not lose

Every business has files it could not replace: the accounts, the customer records, the work itself. The question is whether a second copy exists somewhere that would survive the first being lost, stolen or encrypted. A copy nobody has ever opened is not yet a backup.

F A domain name

The name your website address and email addresses end in. It is held with a company you renew it with. If you cannot say whose name it is in, write that down: that is the answer. Note the renewal date if you know it.

G A website

Anything published under your name, including a single page, an online shop or a booking site somebody else hosts. Count whoever built it if they can still get in.

WHAT EACH LINE MEANS

H Cloud storage

Anywhere work files live other than your own computer: shared drives, file-sharing links, online backups.

I Social accounts

Every account that posts as the business rather than as a person, including ones nobody has used for a year.

J Accounting or payroll software

Anything holding financial or staff records. Include a bookkeeper's system if your data goes into it.

K Staff accounts and logins

Every login held by somebody who works for you, including part-time, casual, seasonal and family. The question is what actually removes access, and on which day: it is often not the day they stop coming in.

L Devices they own themselves

Phones, tablets and laptops the business does not own, with work email or work files on them.

M Card payments or customer records

Anywhere you take card payments, and any personal data you hold about customers. Note anyone else who stores a copy.

N Suppliers with access to your systems

Anyone outside the business who can log in to something of yours: IT support, web developer, bookkeeper, marketing agency, the person who set it all up years ago.

O Software you build or have built

An app, a web app, or a system built for you. Include anything a developer can change and put live without anybody else checking. Whoever can release it can change what your customers run, with your name on it.

P Insurance

Cyber cover, or a business policy with a cyber section. If you have one, the questionnaire you answered forms part of it, so what you said on it matters.

Nothing here needs a technical answer. Every line is a question about what you own and who can reach it, and you are the only person who can answer either.

SOMEONE ELSE CAN GET TO IT

Both are normal and usually right. They fail differently, so they are asked about separately.

IF ANYONE WORKS FOR YOU

Three questions about how the business works. Answer them once, not line by line.

1 What actually removes someone's access on their last day?

Not who intends to. What step does it, and who does that step.

2 Is anything shared rather than individual?

A password several people know cannot be switched off for one of them. It has to be changed for everybody.

3 Does anyone still have access they no longer need?

Access is granted for a reason and outlives it.

FOR EACH SUPPLIER

These are per supplier, not once. Every arrangement is different, and the differences are the point.

1 Whose name is the account in, yours or theirs?

An asset registered in a supplier's name is the supplier's asset, whoever paid for it.

2 Could you get in without them?

Not to cut them out. To find out whether you could if you had to.

3 What can they reach beyond what you hired them for?

Access is granted once and widened quietly.

4 Who at their end has access, and what happens when their staff leave?

Their leaver process is now your leaver process.

5 If they were breached, would you be told, and how fast?

Worth agreeing before it matters.

6 If they stopped answering tomorrow, what would you lose?

Illness, a fallout, a business closing. Not malice, just absence.

One row each, starting with its letter from page two: "E, domain name".

Do not guess, and do not go and find out yet. A blank is more useful than a guess.

Those are your results. Not a stranger's list, and not a list of everything: a list of what you could not answer about your own business.

Initials are fine anywhere a name would go, and a company name is fine for a supplier.

Read it again whenever somebody leaves or a supplier changes. The staff rows say what to switch off; the supplier rows say what you would have to ask for back.

YOU ARE DONE

THREE THINGS, AND THEY ARE YOURS

Take the three blanks from page six that worry you most, and close those this month. Then put the form somewhere you will find it again.

If somebody else needs to see this, pass on the whole form, the list on page six, and those three things. Every line is explained on pages three and four, so it can be read without having sat through the exercise.

Free posters for the wall: kingofcybersecurity.com/royal-armoury

Start with what you have.
The kingdom is fictional. The threats are not.