BEFORE · FROM THE FAAA CONGRESS 2026 PANEL

Make it harder to happen. Eat your cyber vegetables first.

Keep this on paper. When the computers are down, everyone needs to know where this is and what to do. The government's own advice is to keep a copy of your plan offline, in case your systems can't be reached.

Your best line of defence is human. It's people eating their cyber vegetables every day, and if it does happen, people responding in a way that makes sense.

The eight basics. Tick the ones you've done.



1 · BROCCOLI

Turn on MFA (multi-factor authentication)

A stolen password on its own won't get them in.

☐



2 · CARROTS

Automatic updates on

Closes the known holes that old software leaves open.

☐



3 · PEAS

Back up, and test the backups

Get your files back without paying. Keep a copy offline.

☐



4 · PUMPKIN

A password manager

A different password everywhere, so one stolen password doesn't open everything.

☐



5 · BEETROOT

A set process to approve every payment

Two people on every payment, and ring back on a number you already have.

☐



6 · ASPARAGUS

Only the access each role needs

No shared logins. It limits how far one taken-over account can reach.

☐



7 · BRUSSELS SPROUTS

Devices lock themselves; wipe before you sell

A lost or sold device doesn't hand over client files.

☐



8 · MUSHROOMS

A plan for when it goes wrong, practised

Everyone knows the first steps, so a bad day stays smaller. Turn over: the back of this sheet is the start of it.

☐

Under all eight, your people. Stop, check and ask. Ring back on a number you already have.

Count your ticks. The first gap you find is your next job.

The eight basics come from the FAAA Congress panel, "AI for Good, AI for Bad", 26 November 2026, moderated by Morris Misel with James Ng (Insignia Financial) and Rob Smith (NAB), and from the Australian Cyber Security Centre's Small Business Cyber Security Handbook (October 2026). This sheet is Morris Misel's own; it hasn't been reviewed or endorsed by NAB, Insignia Financial or the FAAA.



General information only, not legal, financial or technical advice for your situation. For advice on your own practice, talk to your IT provider, your insurer, your licensee or a lawyer. Checked against official Australian sources on 26 November 2026. Numbers and rules change, so check cyber.gov.au once a year.

Morris Misel
Business Futurist · Keynote Speaker · Author
Founder, Think-Along AI
morrismisel.com · morrismisel.com/join

AFTER · FILL IT IN NOW, PIN IT UP, PRACTISE IT

If it happens. The bad day sheet.

Keep this on paper. If your systems are locked, a plan saved on your computer is locked too. Keep this somewhere everyone knows.

When it happens, we tend to respond emotionally. What we need is a rational response. The middle of an attack is about the worst time to think clearly, so decide it now, while it's quiet.

The first hour

Don't pay, and don't reply to them.
Photograph any ransom message and note the time.

Stop using it, then turn off and disconnect.
Staff stop using affected systems and don't forward the message. Turn off affected devices and unplug them from the network, Wi-Fi and drives, unless your IT provider says otherwise.

Don't wipe anything yet.
No rebuilding or restoring until your IT provider says so. Keep backups unplugged until they're checked clean.

Money involved? Ring your bank now.
Use the number on its website or your card, and ask it to stop the transactions.

Ring your IT provider and your insurer.
Use the insurer's incident line, and check what it must approve before you bring in outside help or spend money.

Change passwords from a clean device.
Email first. Sign out other sessions, turn on MFA, and look for forwarding rules you didn't set.

Write it all down.
What happened, when, and everything you do. Keep the messages.

Email taken over? Ring your clients.
Tell them and your suppliers straight away, and say what you'll never ask them for.

Who to tell

The government's cyber hotline
1300 CYBER1 (1300 292 371), 24 hours, 7 days. Report at cyber.gov.au.

Free help for a small business
IDCARE, **1800 595 170**, Mon to Fri, 8 am to 6 pm AEST, for businesses with an ABN and 19 or fewer full-time-equivalent staff, not counting the owner. Clients whose identity is at risk: **1800 595 160**.

Your licensee
Under your breach process; they decide whether it goes to ASIC. Hold your own licence? Then it's your call, within 30 days.

Client information exposed?
If the Privacy Act covers you (most practices over $3 million turnover, and some under it; ask your licensee), tell the people affected and the OAIC as soon as you can when serious harm is likely. Finish assessing it within 30 days at the most.

Paid a ransom?
If your turnover was about $3 million or more last financial year, you must report it within 72 hours of paying, at cyber.gov.au.

A scam, a threat, a danger
Scamwatch for a scam. Local police for threats. **000** if anyone is in danger.

Fill this in now, while it's quiet

In charge, and deputy _____
IT provider, after hours _____
Insurer incident line _____
Backups, and who restores them _____
How staff raise the alarm _____
Bank fraud line _____
Licensee contact _____
Policy number _____
How we talk if email is down _____
How we keep seeing clients _____

Drill it. Like the armed forces, practise in peacetime so you're ready on the bad day (Rob Smith, NAB, on the panel). Put this sheet in every induction and in your ongoing training, and keep reminding people it's here, so everyone knows what to do and when.



General information only, not legal, financial or technical advice for your situation. For advice on your own practice, talk to your IT provider, your insurer, your licensee or a lawyer. Contacts and rules checked against official Australian sources (ASD's ACSC, IDCARE, OAIC, ASIC, Home Affairs, Scamwatch) on 26 November 2026. They change, so check cyber.gov.au once a year.

Morris Misel
Business Futurist · Keynote Speaker · Author
Founder, Think-Along AI
morrismisel.com · morrismisel.com/join