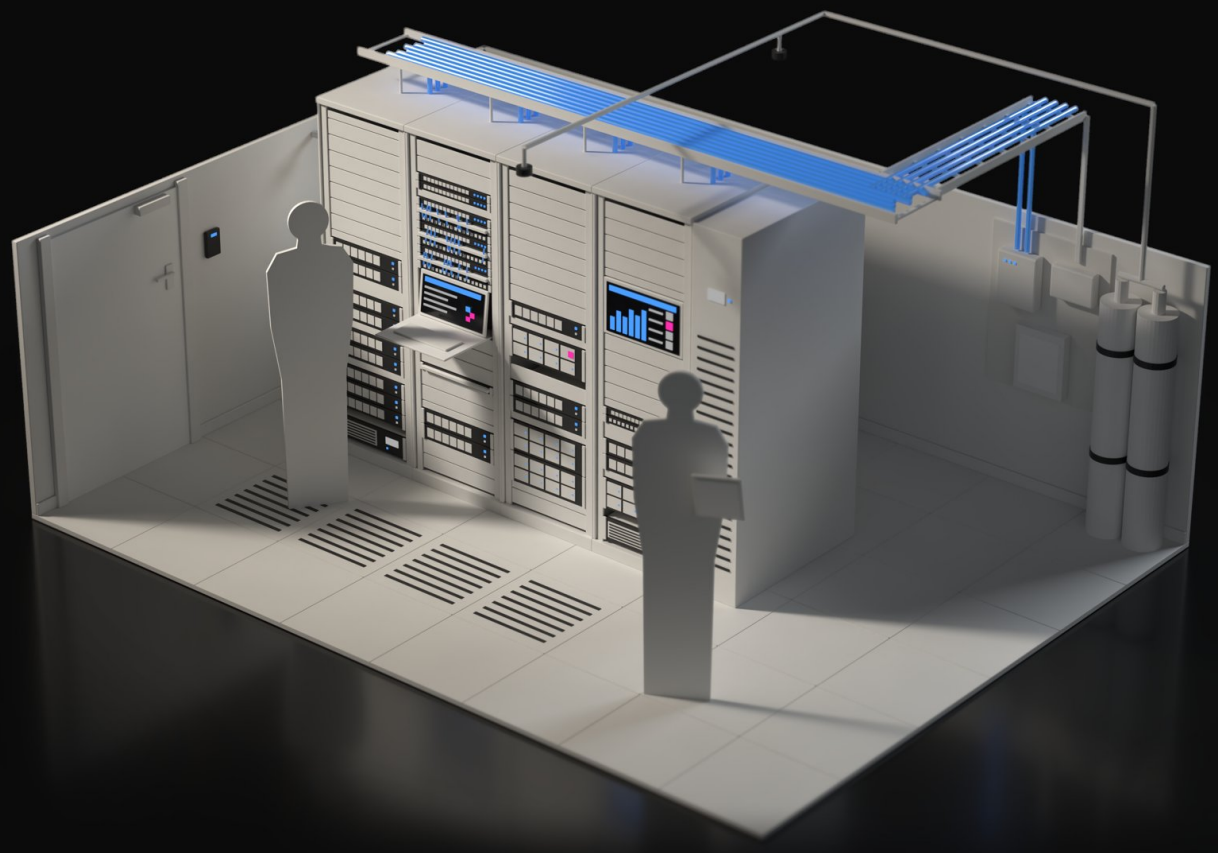


KEEP A PRINTED COPY · AS OF NOVEMBER 2026

Incident response. Simplified.

The first hour after a cyber incident, on one page, plus the numbers you'll need and the reporting deadlines.

John Morgan · Initial Technology · November 2026

THE ONE THING TO KNOW

In the first hour, calm and a plan beat expertise.

Most damage happens because people panic, switch things off, or wait too long to call. Print this, fill it in, and keep it with your insurance policy.

SIMPLIFIED

Contain. Call. Keep a log. Don't switch off. Don't pay without advice. Report on time.

THE FIRST HOUR

01

1. Contain

Unplug network cables and Wi-Fi. Leave devices on.

02

2. Call

IT provider, then insurer, then ASD.

03

3. Log

What happened, who did what, what time.

04

4. Secure accounts

Change passwords from a clean device.

05

5. Brief the lead

One person decides. One voice outside.

06

6. Check deadlines

Data breach and ransom reporting.

NUMBERS TO HAVE READY

FILL IT IN

IT PROVIDER (24/7) _____

CYBER INSURER INCIDENT LINE _____

POLICY NUMBER _____

LAWYER _____

BANK FRAUD LINE _____

INCIDENT LEAD AND DEPUTY _____

ASD HOTLINE: 1300 CYBER1 (1300 292 371) _____

IDCARE: 1800 595 160 _____

STEP 01

Deadlines, simplified

Some of these are law. Diarise them the moment something happens.

- [ ] **Personal information exposed?**
  Assess within 30 days. If serious harm is likely, notify the OAIC and the people affected as soon as practicable.
- [ ] **Ransom paid?**
  Businesses over $3M turnover report to ASD within 72 hours.
- [ ] **Insurer.**
  Most policies require notice straight away, before you engage outside help.
- [ ] **Your board.**
  Tell them early, even if the facts aren't clear yet.

HANDY TIP

'We're still investigating' is an acceptable first message. Silence isn't.

STEP 02

Don't make it worse

The common mistakes, all avoidable.

- [ ] **Don't switch machines off.**
  Evidence in memory disappears.
- [ ] **Don't wipe and rebuild yet.**
  Investigators need to see how they got in.
- [ ] **Don't coordinate by email.**
  Assume it's compromised. Use phones.
- [ ] **Don't talk to the criminals alone.**
  Get expert and legal advice first.

STEP 03

After it's over

The fix isn't finished until the gap is closed.

- [ ] **Find the way in, and close it.**
  Then check for anything left behind.
- [ ] **Restore from clean backups.**
  Most important systems first.
- [ ] **Write a short report for the board.**
  What happened, cost, what changes.
- [ ] **Practise twice a year.**
  A one-hour tabletop exercise is enough.

HANDY TIP

ASD publishes free 'Exercise in a Box' scenarios. Run one with your leadership team before you need it.

WRITE IT DOWN

NEXT PRACTICE RUN _____

RUN BY _____

Want help writing your plan?

I'll turn this page into a plan that fits your club, with your people, your systems and your insurer's rules, and run the first practice with you.

0401 539 456 · info@initialtech.com.au · initialtech.com.au

THE SIMPLIFIED GUIDES

Free at initialtech.com.au/resources

01 Microsoft 365 security

02 Cyber basics and phishing

03 Ransomware readiness

04 Backup and recovery plan

05 Incident response

06 Working from home securely

07 Copilot readiness

08 Choosing an IT provider

09 Buying a major system

10 The board technology report

11 Copilot vs ChatGPT vs Claude

Sources, checked November 2026. OAIC: Notifiable Data Breaches scheme (assessment within 30 days). Cyber Security Act 2024 (Cth), Part 3: ransomware payment reporting within 72 hours. ASD's ACSC: 1300 CYBER1, ReportCyber, Exercise in a Box. IDCARE. General information only, not legal, insurance or financial advice. Check current details with your IT provider before acting.