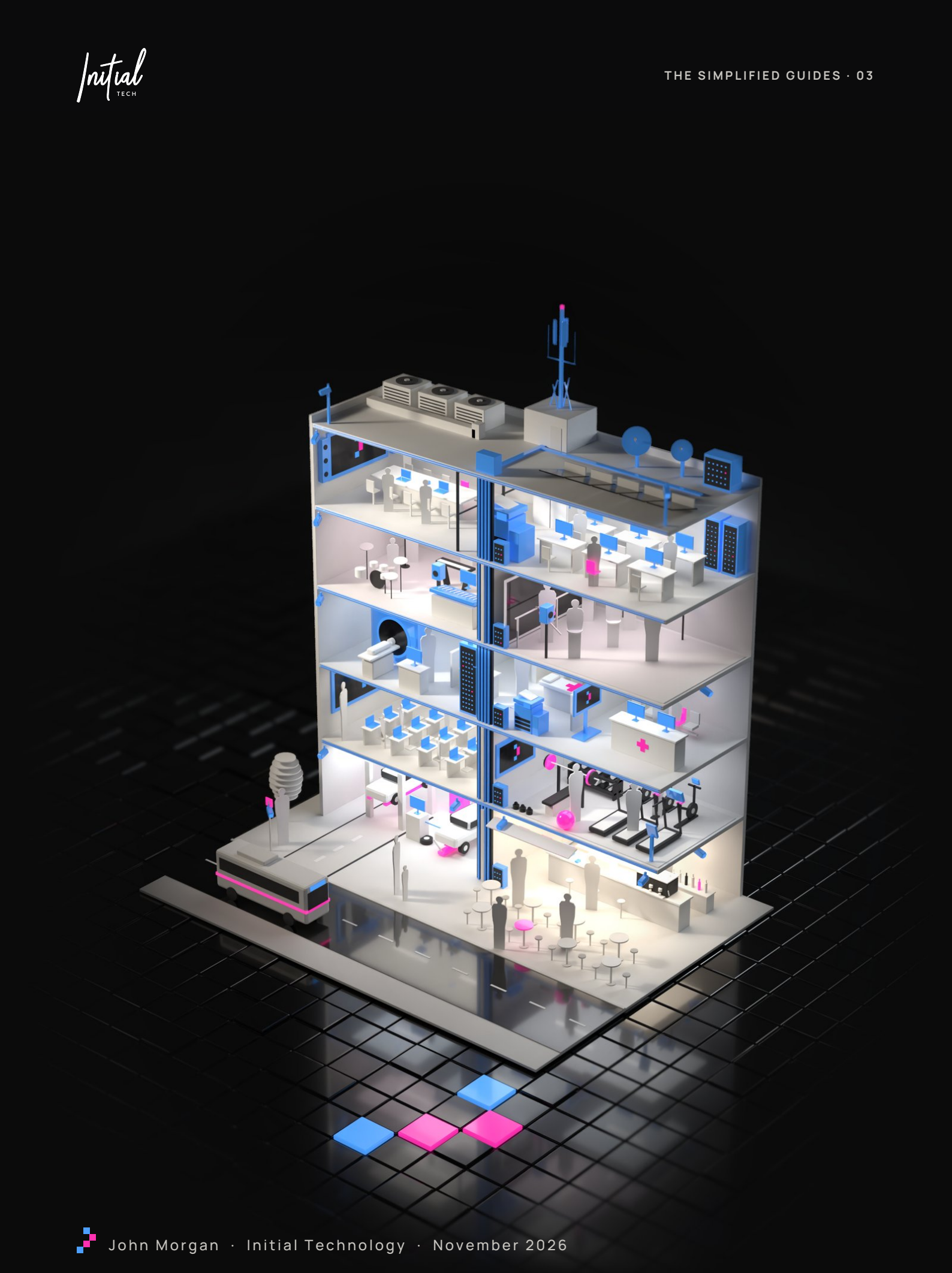


John Morgan · Initial Technology · November 2026

THE ONE THING TO KNOW

The clubs that recover fastest planned for a Friday night.

Ransomware locks your systems and often steals data too. The ones that bounce back have backups criminals can't touch, a plan on paper, and people who know their part.

SIMPLIFIED

Make it hard to get in. Keep a backup they can't reach. Know who decides. Report within 72 hours if you pay.

BEFORE, DURING, AFTER

01

Before: harden

Updates, strong sign-in, few admins.

02

Before: offline backup

A copy that can't be changed.

03

Before: a plan

Who decides, who to call.

04

During: contain

Isolate, don't switch off.

05

During: call

IT, insurer, ASD.

06

After: recover and learn

Restore clean, fix the gap.

THE LAW, SIMPLIFIED

72 hours
to report a ransom payment to ASD

$3M+
annual turnover: the reporting rule applies to you

30 May 2025
the date the rule started

STEP 01

Make it hard to get in

Most ransomware starts with a stolen sign-in or an unpatched system.

- [ ] **Patch internet-facing systems fast.**
  Firewalls, remote access and email first.
- [ ] **Multi-factor everywhere.**
  Especially remote access and admin accounts.
- [ ] **Remove old remote access.**
  Unused VPNs and vendor tools are open doors.
- [ ] **Limit admin rights.**
  Staff don't need to install software.

HANDY TIP

Ask your gaming, CCTV and POS vendors how they connect in remotely, and whether it's protected by multi-factor. Then write down the answer.

STEP 02

Keep a backup they can't reach

If your backups are on the same network, they'll be encrypted too.

- [ ] **One copy offline or locked.**
  Immutable or disconnected, so it can't be changed.
- [ ] **Test a full restore.**
  At least twice a year, timed.
- [ ] **Know the order.**
  Which systems come back first on a trading night.
- [ ] **Protect the backup logins.**
  Separate accounts, multi-factor, few people.

HANDY TIP

Time your restore test. 'We have backups' and 'we can trade again by Saturday' are very different promises.

WRITE IT DOWN

LAST FULL RESTORE TEST _____

TIME IT TOOK _____

STEP 03

Plan who does what

Decisions are hard at 2am. Make them now.

- [ ] **Name the incident lead.**
  Plus a deputy for when they're away.
- [ ] **Decide who talks to members and media.**
  One voice, approved words.
- [ ] **Know your insurer's rules.**
  Many require you to call them before anyone else.
- [ ] **Agree the ransom position.**
  ASD advises not to pay. Decide with your board now, not during.

WRITE IT DOWN

INCIDENT LEAD _____

DEPUTY _____

INSURER'S INCIDENT LINE _____

STEP 04

If it happens

Contain first, then call for help.

- [ ] **Disconnect, don't switch off.**
  Pull network cables and Wi-Fi. Leave machines on for the investigators.
- [ ] **Don't use email to coordinate.**
  Assume it's being watched. Use phones.
- [ ] **If a ransom is paid:**
  Businesses over $3M turnover must report it to ASD within 72 hours.
- [ ] **Call your IT provider and insurer.**
  Then ASD on 1300 CYBER1 (1300 292 371).
- [ ] **Check what data was taken.**
  Personal information may mean notifying the OAIC and members.
- [ ] **Keep a log.**
  Who did what, and when. Insurers and regulators will ask.

HANDY TIP

Print this page and keep it with the insurance policy. When systems are down, a PDF on the server doesn't help.

Want to know if you'd recover?

A ransomware readiness review tests your backups, your remote access and your plan, and tells the board in plain English how long you'd be down.

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. Cyber Security Act 2024 (Cth), Part 3, and Cyber Security (Ransomware Payment Reporting) Rules 2025: reporting within 72 hours for businesses with turnover over $3 million, from 30 May 2025. ASD's ACSC: ransomware guidance and 1300 CYBER1. OAIC: Notifiable Data Breaches scheme. General information only, not legal, insurance or financial advice. Check current details with your IT provider before acting.