ALL I.T

A FREE PRACTICAL RESOURCE FOR STRATA OWNERS & MANAGERS

Strata Ransomware Checklist

The questions every strata committee, building manager and agency should be asking their IT provider right now.

VERSION 1.0 • APRIL 2026 • ALLITSERVICES.COM.AU

01 — WHY THIS CHECKLIST EXISTS

A wake-up call from inside the industry.

In April 2026, a NSW-based strata management company was compromised by the Kairos ransomware group. The attackers claimed to have stolen roughly **441 GB** of data — including resident records, financial details and building documentation — and published the files online when the ransom was not paid.

Strata holds a dense concentration of exactly what criminals are looking for: bank accounts, identity documents, levies, maintenance contracts, access records, insurance policies, and contact details for hundreds or thousands of lot owners per scheme. Most schemes run their operations through a small number of core platforms, many of them online, and many of them shared between owners, managers, committees and contractors.

> **THE HARD TRUTH**
>
> If a single strata manager's credentials are stolen, an attacker can potentially reach every lot, every owner and every trust account they administer. That is why strata is now a priority target — and why every scheme needs to be asking sharper questions of its IT.

WHO THIS CHECKLIST IS FOR

- **Strata managers and agencies** responsible for multiple schemes.
- **Owners corporations, executive committees and chairs** who want to verify their manager's controls.
- **Building managers and facilities teams** handling access systems, CCTV and IoT.
- **Lot owners** who want to understand the risk to their personal and financial information.

HOW TO USE IT

Work through each section in order. Tick the items you can verify today. Anything left unticked is a question to put to your IT provider, your strata manager, or both. If you are the IT provider — use it as a self-audit.

Five reasons attackers love this industry.

1 Dense personal and financial data

Owner identity details, levy payments, bank data, insurance policies, tenancy and access records — all in one place.

2 Shared access, many hands

Owners, committees, contractors, managers and building staff all have some kind of access to systems and documents.

3 Trust accounts and real money

Strata trust accounts move millions of dollars. Invoice fraud and payment redirection are highly profitable attacks.

4 Legacy and cloud, side by side

Most agencies run a mix of on-prem, legacy and SaaS systems — which creates seams attackers love to exploit.

5 Reputation and regulation

Privacy Act 1988 and the OAIC Notifiable Data Breach scheme apply — a breach is not just technical, it is a public event.

Identity & access.

Most ransomware attacks begin with a stolen or guessed password. Start here.

- [ ] **Multi-factor authentication (MFA)** is enforced on every email account, every platform login and every remote-access tool — no exceptions for executives or senior staff.
- [ ] **Phishing-resistant MFA** (app-based, hardware keys or number-matching) is used, not SMS codes.
- [ ] **Password manager** is provided to all staff; credentials are never shared in chat, spreadsheets or email.
- [ ] **Joiner-mover-leaver** process exists: access is removed the same day a person leaves or changes role.
- [ ] **Privileged accounts** (admin, finance, trust account signers) are separated from day-to-day user accounts.
- [ ] **Conditional access** blocks logins from unusual countries, unknown devices and risky IPs.
- [ ] **Service accounts and API keys** are inventoried, rotated and not shared between platforms.

Core strata applications.

PropertyIQ, StrataMax, Strata Master, MYBOS, BuildingLink, Urbanise — whatever you run, these questions apply.

- [ ] Every core platform enforces **MFA** and logs all administrator actions.
- [ ] **Role-based permissions** are reviewed quarterly — not every user needs access to every scheme.
- [ ] Vendor integrations (document portals, payment gateways, owner portals) use **scoped API tokens**, not shared admin logins.
- [ ] You have written confirmation of each vendor's **data hosting location**, backup policy and breach-notification process.
- [ ] **Single sign-on (SSO)** is used where the platform supports it, so one leaver revokes access everywhere.
- [ ] **Session timeouts and device trust** are configured — not just "remember me forever".
- [ ] Exports of owner and financial data are **logged and alerted on** — not silent.
- [ ] You know who to call at each vendor in a breach — 24×7, not just a support ticket.

Email, invoices & trust accounts.

Business email compromise and invoice redirection are where most strata money actually goes missing.

- [ ] **DMARC, SPF and DKIM** are fully configured on every domain you send from — enforced, not monitor-only.
- [ ] **External sender warnings** are on; look-alike domains are blocked or quarantined.
- [ ] **Bank detail changes** for suppliers and contractors require a phone call-back on a known number — never email-only.
- [ ] **Dual authorisation** is required for trust account transfers over an agreed threshold.
- [ ] **Payment runs** are reviewed against source invoices, not just against the last run.
- [ ] **Forwarding rules** (auto-forward to external addresses) are blocked or alerted on across the whole tenancy.
- [ ] **Owner and committee comms** use a known, branded sending domain — not a personal Gmail or Outlook account.

Devices, endpoints & the office.

Laptops and phones are where the first click usually happens. They need to be managed, not trusted.

- [ ] Every laptop, desktop and phone used for work is **enrolled in a management platform** (Intune, Jamf, Kandji or equivalent).
- [ ] **Endpoint Detection and Response (EDR)** is installed and monitored — not just traditional antivirus.
- [ ] **Disk encryption** (BitLocker, FileVault) is on by default.
- [ ] **Operating systems and browsers** patch automatically on a monthly cycle, with compliance reporting.
- [ ] **USB and removable media** controls are in place — especially for finance and reception machines.
- [ ] **Personal devices** used for work (BYOD) are either blocked or fenced into a managed app area.
- [ ] Lost or stolen devices can be **remotely wiped** — and someone knows how to actually do it.

Backups, recovery & business continuity.

The difference between a bad week and a business-ending event is almost always the backups.

- [ ] Backups follow a **3-2-1 rule**: three copies, two different media, one off-site and offline or immutable.
- [ ] **Immutable** or air-gapped backups exist — attackers cannot delete them with stolen admin credentials.
- [ ] Backups include your **Microsoft 365 or Google Workspace** data — email, SharePoint, OneDrive, Teams.
- [ ] **Restore tests** are run at least quarterly — not just when you need them.
- [ ] You have a written **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** for each critical platform.
- [ ] A **business continuity plan** covers how trust accounts, levies and resident comms keep running if your core platform is down for a week.
- [ ] Key contacts, insurance policies and vendor escalation numbers are stored **outside** the systems you'd be locked out of.

Governance, people & response.

Controls are only as good as the humans who run them — and the plan for the day something goes wrong.

- [ ] **Security awareness training** runs at least annually, with simulated phishing at least quarterly.
- [ ] Staff know **how to report** a suspicious email or call — and reporting is encouraged, not punished.
- [ ] A written **incident response plan** exists — and at least one tabletop exercise has been run in the last 12 months.
- [ ] **Cyber insurance** is current and you have confirmed what it actually covers for strata data and trust accounts.
- [ ] You know your obligations under the **Privacy Act 1988** and the **OAIC Notifiable Data Breach** scheme.
- [ ] **Committees and owners** are briefed on what data is held, where it is held, and who can access it.
- [ ] The **Essential Eight** (ACSC) maturity level for the agency is known, documented and being improved.

04 — STRATA PLATFORMS

The platforms we see every day.

Whatever you run, the controls above apply. Here are the stacks we see across Australian strata clients.

CORE STRATA MANAGEMENT

- PropertyIQ (PIQ)
- StrataMax
- Strata Master
- Rockend

BUILDING & FACILITIES

- MYBOS
- BuildingLink
- Urbanise

OWNER & RESIDENT PORTALS

- Vendor-branded portals
- Document repositories
- Voting & meeting platforms

PRODUCTIVITY & COMMS

- Microsoft 365 / Google Workspace
- DocuSign and similar
- Accounting integrations

> Running something not listed here? That's fine — we work across the full Australian strata stack. The questions in this checklist still apply.

ALL I.T

NEXT STEP

Want someone to run through this with you?

We work with strata agencies, owners corporations and building managers across Australia. If anything in this checklist left you unsure, book a free 30-minute review with our team — no pitch, no obligation, just a straight answer on where you stand.

BOOK A FREE STRATA IT REVIEW

---

allitservices.com.au/strata-ransomware-checklist

1300 ALL IT · hello@allitservices.com.au

All IT is an Australian Managed Service Provider, founded 2005. We deliver secure IT, cyber-security and infrastructure management to clients across strata, hospitality, financial services and beyond.