

AdvancedBITS | Business IT Solutions

Why Real Estate Management Should Consider AdvancedBITS

A practical case for property management and real estate firms that want secure, reliable, and scalable technology, without building a large internal IT department

Executive takeaway

Real estate management firms should consider AdvancedBITS if they want a technology partner that treats payment fraud, tenant data, recovery, and growth as one operating discipline. Property managers hold identity data, move money constantly, and depend on many vendors and mobile staff. Break/fix support and a stretched internal team struggle to cover that alone, and 24/7 monitoring cannot be staffed by one or two people. AdvancedBITS provides managed or co-managed IT, cybersecurity, Microsoft 365 governance, backup and recovery, and AI readiness, backed by more than 11 years of managed services experience and evidence you can hand to an insurer, owner, or lender.

The short answer: when AdvancedBITS is a good fit

Consider AdvancedBITS if two or more of the statements below describe your firm. They are the situations where property management companies most often decide a managed technology partner is worth it.

- Your IT is one or two people, or a break/fix vendor, and they spend most of their time on tickets.
- You manage multiple properties or offices, and staff work from sites, leasing offices, vendors, and home.
- Payment changes, owner distributions, or deposits are approved by email, and the process is not written down.
- You could not answer a cyber insurance questionnaire, or an owner or lender security review, with evidence.
- You have never test-restored a backup, so you do not know how long recovery would take.
- You are adding properties through acquisitions and want a repeatable technology baseline.
- Staff are already using AI tools, and no one has defined approved tools or prohibited data.

If none of these apply, and you already run a mature, staffed, 24/7 security operation, a co-managed arrangement for specific gaps may fit better than full management. We will tell you that during the assessment.

Why the decision matters more now

Property management combines three things attackers want: identity data, payment activity, and many third parties. Independent research shows the exposure is growing and that most attacks succeed through people and identity, not exotic software flaws.

Table 1. What independent research shows

Finding	Source
Real estate fraud complaints to the FBI reached 12,368 in 2025 with reported losses of \$275 million , up from 9,359 complaints and about \$173 million in 2024. The FBI category includes real estate investment, rental, and timeshare fraud, so it is broader than closing wire fraud.	FBI Internet Crime Complaint Center (IC3) 2025 Annual Report, as reported by NAR REALTOR Magazine (April 2026)
Business email compromise (BEC) and funds transfer fraud made up 58% of all cyber insurance claims. The average funds transfer fraud claim was \$112,000 , and 71% of those claims involved social engineering.	Coalition 2026 Cyber Claims Report (March 2026; 100,000+ policyholders)
Malicious email (26%) and phishing (24%) were the top two root causes of ransomware attacks, and 79% of attacks began with an identity-based approach. Average recovery cost was \$1.7 million .	Sophos State of Ransomware 2026 (July 2026; 2,158 organizations that were hit)
Real estate leaders recognize the risks but are “still working through how to respond.” Deepfake voicemails mimicking executives are being used to request urgent wire transfers, and smart building systems expand the attack surface.	RSM US, MMBI Cybersecurity Special Report (May 2026)

FBI figures are complaints reported to the FBI, so actual losses are likely higher. Coalition and Sophos figures reflect insured policyholders and organizations that were hit. Sophos surveyed organizations of 100 to 5,000 employees.

Recent incidents show the same pattern. In 2026, Cushman & Wakefield confirmed a limited data security incident due to voice phishing, and Fulcrum Real Estate Services reported ransomware that affected a cloud file-sharing platform and involved the names and Social Security numbers of 1,547 individuals. Details come from company statements, regulatory filings, and news and law-firm summaries. Attacker claims are unverified and no AdvancedBITS involvement is implied.

Seven reasons real estate management firms choose AdvancedBITS

Table 2. What you get and how it works

Reason	What it means for your firm	How AdvancedBITS delivers
1. Built for multi-site, mobile teams	Leasing offices, field staff, and vendors all need secure access without slowing down service.	Managed laptops, tablets, and phones, secure remote access, a help desk that understands multi-site operations, and fast onboarding and offboarding.

Reason	What it means for your firm	How AdvancedBITS delivers
2. Payment fraud defense, not just software	Technology reduces fake emails, but only a written procedure stops the ones that get through.	Email security and domain protection, MFA, mailbox monitoring, staff training, and a written call-back and dual-approval rule for payment and bank-detail changes.
3. Evidence for insurers, owners, and lenders	Brokers report underwriters expect proof of MFA, endpoint detection and response, tested backups, a tested incident response plan, and vendor oversight.	Cyber insurance readiness assessments, security policies, vendor access reviews, and an evidence file you can hand to your broker.
4. Recovery you have actually tested	Recovery time protects rent collection, work orders, and accounting.	Backup and disaster recovery with documented restore tests and a continuity plan.
5. Microsoft 365 and AI governance	Tenant records, leases, and owner reports live in SharePoint, Teams, and OneDrive, and AI tools can surface whatever staff can open.	Permission, guest access, and sharing reviews, plus AI acceptable use rules and human review standards before any rollout.
6. A model that fits how you run	Some firms want IT handled end to end. Others want to keep an internal lead.	Fully managed or co-managed engagements, with responsibilities written down before day one.
7. A roadmap and a predictable budget	Growth and acquisitions create surprise IT costs and inconsistent environments.	Technology reporting, asset management, documentation standards, budget forecasting, and a 12-month roadmap.

Experience and assurance. AdvancedBITS has more than 11 years of managed services experience and a SOC 2 Type II examined security practice. Our clients include organizations in property management and hotel management, among other industries.

Comparing the ways real estate firms handle IT

Most property management firms use one of four models, and each has a known failure mode. The right choice depends on how much internal capacity you have and how much risk you can staff around.

Table 3. IT support models for property management firms

Model	Where it works	Where it falls short
Break/fix vendor	Occasional projects and one-off repairs.	Reactive by design. Problems are handled after damage is done, costs spike during incidents, and no one owns monitoring, security, or planning.
Internal IT only	Firms with a mature, staffed team and floor presence at each site.	One full-time employee works roughly 2,080 of a year's 8,760 hours, so nights, weekends, and vacations go uncovered. Knowledge leaves when a person does.

Model	Where it works	Where it falls short
Co-managed IT	Firms that want to keep an internal lead and add 24/7 monitoring, security, patching, and strategy.	Fails when ownership is vague, so responsibilities and tools must be assigned in writing before the engagement starts.
Fully managed IT (AdvancedBITS)	Firms without internal IT, or with a team stretched too thin, that want one accountable partner for operations, security, recovery, and planning.	Requires trust and clear communication. We address this with named contacts, regular reviews, and documentation you own.

Model descriptions reflect common industry guidance on managed and co-managed IT. Hours are simple arithmetic: 40 hours x 52 weeks is 2,080, and a year has 8,760 hours.

What a single incident can cost

The business case is easiest to see by looking at what one event costs. The figures below are third-party averages, not predictions for your firm, and they show why prevention and tested recovery are usually the cheaper path.

Table 4. Reference points for the cost of doing nothing

Event	Reference point	Source
Funds transfer fraud claim	Average claim of \$112,000	Coalition 2026 Cyber Claims Report
Ransomware recovery	Average recovery cost of \$1.7 million	Sophos State of Ransomware 2026
Real estate fraud, nationwide	\$275 million in reported 2025 losses	FBI IC3 2025, via NAR
Breach notification	Florida: notice to individuals within 30 days. Texas: individual notice within 60 days and Attorney General notice within 30 days when 250 or more Texans are affected.	Florida Statutes 501.171 and Texas breach-law summaries

Insurance claims and survey averages vary widely. Breach-law details are general information and not legal advice. Confirm requirements with counsel for every state where you manage properties.

What the first 90 days look like

You see progress on a fixed timeline, and each phase ends with evidence. The roadmap matches the one in our property management cybersecurity case study.

Table 5. 90-day start

Phase	What happens	What you get
Days 1 to 30: Assess	Review identity, Microsoft 365, endpoints, backups, vendor access, payment-change procedures, and AI use. Enforce MFA on the highest-risk accounts.	A prioritized risk report, a plain-language summary for leadership, and a written payment-verification rule.

Phase	What happens	What you get
Days 31 to 60: Secure	Deploy endpoint and email protections, manage field devices, tighten permissions, and segment building and camera networks.	The highest-risk gaps closed and documented.
Days 61 to 90: Prove and plan	Test a restore, train staff, publish an AI acceptable use policy, document an incident response plan, and build a 12-month roadmap.	Evidence for insurers, owners, and lenders, plus a budgeted plan.

Questions to ask any managed IT provider

Use this checklist with AdvancedBITS and with any other provider you evaluate. Specific answers are a better sign than confident ones.

Table 6. Provider evaluation checklist

Ask	A strong answer sounds like
Who owns monitoring after hours, and what is the response commitment?	A named process, written response targets, and an escalation path, not “we will see the alert in the morning.”
How do you reduce payment fraud for a firm like ours?	Technical controls plus a written callback and dual-approval procedure, and staff training.
Can you show a restore test, and how long did it take?	A documented test with a measured recovery time.
Do you have independent assurance of your own security?	A current third-party report, such as a SOC 2 Type II examination, that you can request.
Who owns the documentation and credentials?	You do. The provider shares them in a shared, audited system.
How will you work with our internal IT lead, if we have one?	Written responsibilities, shared tools, and one ticketing system.
How do you handle vendor and PropTech access?	An inventory, least-privilege accounts, and periodic access reviews.
What happens at the end of the engagement?	A clear exit process and handover of documentation.
How do you price, and what is excluded?	Transparent scope tied to users, devices, and sites, with projects and exclusions listed.

What independent research says about the controls we recommend

These are third-party benchmarks, not AdvancedBITS client results.

Table 7. Independent research benchmarks

Control area	Independent finding	Source
Multi-factor authentication and security controls	99.22% reduction in account-compromise risk	Microsoft Research (May 2023)
Security awareness training	87% reduction in Phish-Prone Percentage after 12 months of training	KnowBe4 2026 Phishing by Industry Benchmarking Report
Cloud-based disaster recovery	67% faster recovery	2026 aggregated disaster recovery statistics
Identity and access management improvements	80% reduction in new-user onboarding time	Infosys financial-services case study

Results vary by environment. The onboarding benchmark comes from financial services and is included because property teams onboard leasing, maintenance, and seasonal staff often.

Learn more

- **Managed IT and cybersecurity for property management:** our commercial overview of services, incidents, and the free assessment.
- **Property Management Cybersecurity and Managed IT case study:** a composite 90-day scenario with a before-and-after scorecard.
- **AI in Real Estate Management case study:** how a firm governs Microsoft 365 and prepares for responsible AI.

Frequently asked questions

Why should a property management company use a managed IT provider?

Most firms cannot staff round-the-clock monitoring, patching, Microsoft 365 governance, and security documentation internally. A managed provider supplies those capabilities, plus a roadmap, at a predictable cost that scales with the portfolio.

Do we have to replace our internal IT person?

No. A co-managed model keeps your internal lead in charge of local support and strategy, while AdvancedBITS covers 24/7 monitoring, security, patching, backup, and planning. Responsibilities are written down before day one.

What is the difference between managed and co-managed IT?

In fully managed IT, the provider acts as your IT department. In co-managed IT, your internal team stays and the provider fills gaps such as security monitoring, escalation, and strategic planning.

How much does managed IT cost for a property management firm?

Pricing depends on users, devices, sites, and scope. We provide a written proposal after the free assessment, with inclusions and exclusions listed, so you can compare it with your current spend and risk.

Can AdvancedBITS support Yardi, AppFolio, Buildium, RealPage, or Entrata?

We support the environment around your property management, accounting, and leasing platforms: Microsoft 365, identity, endpoints, mobile devices, networks, backup, and vendor access. During the assessment we review how your platforms integrate and what the vendor is responsible for.

How does AdvancedBITS help prevent wire fraud?

We combine email security, MFA, mailbox monitoring, and training with a written call-back and dual-approval procedure for any change to payment instructions. The FBI logged \$275 million in real estate fraud losses in 2025.

How quickly can we see results?

A focused 90-day program addresses the highest risk gaps and produces evidence such as a restore test, written plans, and a roadmap. Ongoing managed operations follow.

Is it safe to use AI tools in our property management business?

It can be, with controls. We start with Microsoft 365 permissions and property document organization, define approved tools and prohibited data, require human review of anything sent to tenants or owners, and pilot a few workflows before expanding.

Ready to strengthen operations, security, and portfolio performance?

Schedule your complimentary Real Estate Management Technology & Risk Assessment.

We will review cybersecurity readiness, payment-change procedures, Microsoft 365 governance, backup and recovery, vendor access, cyber insurance readiness, and AI use, then give your leadership a prioritized summary with no obligation.

Call 561-300-3015 | sales@advancedbits.com | www.advancedbits.com

AdvancedBITS | Business IT Solutions. Helping real estate and property management organizations strengthen cybersecurity, improve operational efficiency, support compliance, and grow with confidence.

Sources

Statistics and legal summaries were checked against the sources below as of October 22, 2026. This page is general information and not legal advice.

1. FBI IC3. Annual Reports, including the 2025 IC3 Annual Report (April 2026). <https://www.ic3.gov/AnnualReport/Reports>
2. NAR REALTOR Magazine. Online Real Estate Fraud Climbed to \$275M in 2025, FBI Says (April 13, 2026). <https://www.nar.realtor/news/real-estate-news/online-real-estate-fraud-climbed-to-275m-in-2025-fbi-says>
3. RISMedia. FBI Report: Real Estate Fraud Losses Total \$275 Million-Plus in 2025 (April 13, 2026). <https://www.rismedia.com/2026/04/13/report-real-estate-fraud-losses-over-million-2025/>
4. Coalition. 2026 Cyber Claims Report (March 5, 2026). <https://www.coalitioninc.com/claims-report/2026>
5. Sophos. The State of Ransomware 2026 (July 15, 2026). <https://www.sophos.com/en-us/blog/sophos-state-of-ransomware-2026>
6. RSM US. Cybersecurity is becoming a core risk issue for real estate organizations (May 13, 2026). <https://rsmus.com/insights/industries/real-estate/2026-cybersecurity-mmbi-real-estate-snapshot.html>

7. Propmodo. The Cushman & Wakefield Cyberattack Is a Wake-Up Call for Commercial Real Estate (July 1, 2026). <https://propmodo.com/the-cushman-wakefield-cyberattack-is-a-wake-up-call-for-commercial-real-estate/>
8. ClaimDepot. Fulcrum Real Estate Data Breach Exposes Social Security Numbers (updated August 13, 2026). <https://www.claimdepot.com/data-breach/fulcrum-real-estate-services-2026>
9. Florida Statutes. 501.171, Security of confidential personal information. http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/Sections/0501.171.html
10. Recording Law. Texas Data Breach Notification Laws: Reporting Rules and Timelines (reviewed August 28, 2026). <https://www.recordinglaw.com/us-laws/data-privacy-laws/texas-data-privacy-laws/data-breach-notification/>
11. Z Cyber. Cyber Insurance Requirements 2026: The Controls Underwriters Actually Check (August 28, 2026). <https://www.ztekyber.com/resources/cyber-insurance-requirements-2026>
12. UDT. Managed IT vs. Co-Managed IT: Choosing the Right Support Model for 2026 (February 11, 2026). <https://udtonline.com/managed-it-vs-co-managed-it-choosing-the-right-support-model-for-2026/>
13. MSP Directory. Co-Managed IT: When the Hybrid Model Beats Full Outsourcing (June 11, 2026). <https://mspfinders.com/blog/co-managed-it-when-hybrid-beats-full-outsourcing>
14. Microsoft Research (May 2023); KnowBe4 2026 Phishing by Industry Benchmarking Report; 2026 aggregated disaster recovery statistics; Infosys financial-services case study (benchmarks in Table 7).