

Why Should Public Entities Consider Hiring a Managed Services Provider?

The signs, the evidence, what a managed partner adds, and when it is not the right answer

By AdvancedBITS | Business IT Solutions • About 9 minutes to read

Quick answer: should a public entity hire a managed services provider?

A public entity should consider a **managed services provider (MSP)** when its technology depends on one person, important projects stay unfinished, cybersecurity needs outgrow its staff, costs are unpredictable, or recovery has never been tested. An MSP supplies a team, documented procedures, security monitoring, backup and recovery testing, and regular reporting. It does not replace leadership oversight, and it is not a guarantee against attack. We did not find a published study that measures local governments before and after hiring an MSP, so this paper makes the case on evidence you can check and says where the evidence stops.

Technology now sits under permitting, utility billing, records, payroll, public safety communications, and resident services. When it fails, the public notices. The question for leaders is not whether technology matters, but whether the organization has the people, documentation, and oversight to keep it running and protected.

AdvancedBITS is a managed services provider, so read this with that in mind. Statistics are linked and labeled by strength, reasoning is marked as reasoning, and we say when hiring a provider is the wrong call. For what we do day to day, see [Managed IT and Cybersecurity for Public Entities](#).

General information about technology risk. It is not legal, procurement, or compliance advice. Your counsel and procurement office decide which rules apply to your entity.

What does the evidence say about local government IT and cybersecurity?

Short answer: The evidence explains why local governments struggle and why some outsource, but it does not show that outsourcing improves outcomes.

We did not find a published study that measures local governments before and after hiring an MSP. A 2025 academic paper on this topic describes empirical research on how local governments decide to outsource cybersecurity as extremely limited. What exists is research on the pressures behind the decision and on why organizations get hit. Each statistic appears once, here.

Finding	Source	Strength and limits
Interviews with local government officials found no single driver of the decision to outsource cybersecurity. Several drivers combine, and the paper notes that a lack of skills is pushing local governments to contract out.	Waltz and Gasco-Hernandez, SUNY Albany, HICSS 2025 .	Peer-reviewed conference paper based on interviews. Qualitative, so it shows reasons, not results.
Among 3,400 IT and security leaders whose organizations were hit by ransomware, the most common operational factors were a lack of expertise (40.2%), security gaps the organization did not know about (40.1%), and a lack of people or capacity (39.4%). Victims cited 2.7 contributing factors on average. Exploited vulnerabilities were the top technical cause (32%).	Sophos, State of Ransomware 2025; whitepaper .	Survey commissioned by Sophos, which sells security services, and run by a third party. Organizations of 100 to 5,000 employees in 17 countries, all industries, all ransomware victims. Not specific to government.
29% of city and county IT executives said elected officials are very engaged in cybersecurity efforts.	Public Technology Institute, 2024 survey .	Small sample: 54 of 200 executives contacted, July to August 2024. Directional only.

What do recent city and housing authority cases show?

Short answer: In each case, recovery depended on outside help and on facts that took time to establish. That says something about capacity, but it does not prove what any provider would have changed.

- **St. Paul, Minnesota (July 2025).** The city's own report says it detected suspicious activity on July 25 involving [compromised accounts tied to a critical backup server](#). It disabled VPN access for most employees on July 27 and shut down the broader network on July 28. The city requested the Minnesota National Guard's cyber protection support because [the impact exceeded its incident response capacity](#). After the city refused to pay a ransom, data from a Parks and Recreation drive was exposed: about 43 GB, with personal information on 12,484 people, including Social Security numbers. [Smart Cities Dive reports](#) the city spent months recovering.
- **Foster City, California (March 2026).** NBC Bay Area reported that city staff [detected ransomware on March 19](#), that almost all employees were working from home, many customer services were shut down, a state of emergency was declared, and independent cybersecurity experts were brought in. Police emergency lines were briefly down and then restored. Smart Cities Dive later reported that most city services were frozen for weeks.
- **Vicksburg, Mississippi (October 2026).** The city [disclosed a ransomware attack on October 1](#). Police, fire, and 911 were unaffected, but the water and gas department could not look up accounts or take payments, and the city paused late fees and disconnections. [The Vicksburg Post reported](#) on October 19 that the city had missed a billing cycle and hoped to restore systems within days. The board ratified a \$13,600 agreement with two firms to investigate and help restore systems, an estimate the paper says may not reflect the total cost of recovery.
- **Housing authorities.** An insurance executive told a May webinar that attackers are not targeting housing authorities as such, [“they’re targeting opportunity”](#), and that authorities hold deep stores of resident data with limited resources. One housing commission found attackers had been in its systems for three or four months before its 2020 breach.

One more fact keeps this honest. When the District of Columbia Housing Authority was disrupted in 2026, it said it already followed industry standards that included round-the-clock threat monitoring, multifactor authentication, layered email security, and endpoint protection. Controls reduce risk. They do not remove it, and no provider can promise otherwise.

What are the signs it may be time to consider an MSP?

Short answer: When technology depends on one person, projects stay unfinished, cybersecurity has outgrown the staff, costs are unpredictable, documentation is thin, or recovery has never been tested.

This table is AdvancedBITS reasoning, drawn from what public entities commonly tell us. It is not research. Use the last column as a self-test.

Sign	What it looks like	Question to ask yourselves
Technology depends on one person	One employee, consultant, or vendor holds the passwords, configurations, and vendor relationships.	If that person retired or could not be reached in an emergency, who could restore service?
Important projects stay unfinished	Support requests crowd out security upgrades, Microsoft 365 cleanup, documentation, and recovery planning.	Which projects have sat on the list for more than a year?
Cybersecurity has outgrown the staff	Monitoring, patching, and incident response need coverage nights and weekends, plus specialized skills.	Who responds at 2 a.m., and who checks that patches were applied?
Costs are unpredictable	Emergency purchases, aging equipment, and multiple vendors make the budget hard to forecast.	Can your board see a multi-year technology plan and budget?
Documentation is thin	Network diagrams, inventories, and recovery steps are out of date or live in one person's head.	Could a new person run the environment from the documents alone?
Recovery has never been tested	Backups exist, but no one has restored critical systems against a clock.	How long would it take to restore your financial and records systems?

What does an MSP add, and how can you verify it?

Short answer: Coverage, specialization, consistency, and documentation, and every item below should come with evidence you can read.

This is also AdvancedBITS view, not research, and each row says how to check it. An example of the work in sequence is in [Public Sector IT Case Study: Employee Onboarding and Security at a Public Agency](#).

Area	What a managed partner adds	How you verify it
Team coverage	Help desk, after-hours response, and backup staff when someone is out.	Staffing and escalation steps in the contract, and response reports.
Security monitoring and patching	Monitoring, scheduled patching, vulnerability management, and endpoint and email protection.	Monthly security and patch reports, and a named responder.
Identity and Microsoft 365	Multifactor authentication, conditional access, role-based access, and permission and sharing review.	Coverage reports by user and system, and access reviews.
Backup and recovery	Monitored backups, an offline or immutable copy, and scheduled restore tests.	Restore test records with times against a target.
Vendor and third-party access	An inventory of who can reach your systems or host your services, with multifactor authentication and logging.	A vendor access list with review dates.
Documentation and key-person risk	Current diagrams, inventories, runbooks, and shared coverage.	You can read the documents without the provider in the room.
Planning and reporting	A roadmap, asset lifecycle plan, budget forecast, and monthly, quarterly, and annual reports.	Reports leadership can read and act on.
Incident readiness	A written incident plan, contact list, and a rehearsal.	A tabletop exercise record with the date and lessons.

How does managed IT support fiscal stewardship and accountability?

Short answer: By replacing emergency spending with a plan your board can see, and by measuring results against a baseline you set.

- **Plan instead of reacting.** A roadmap, asset tracking, and lifecycle planning turn surprise replacements into scheduled ones.
- **Predictable budgeting.** A defined monthly scope plus planned projects is easier to forecast than emergency repairs. Confirm what the monthly fee includes and excludes.
- **Measured, not promised.** AdvancedBITS records a baseline at the start and re-measures at 90 days: discover and document in days 1 to 30, close the highest-risk gaps in days 31 to 60, then test restores and report in days 61 to 90. The plan is an illustrative AdvancedBITS framework, not a published standard.
- **Reporting.** Monthly reports, quarterly reviews, and an annual assessment give leadership visibility. What to require in a contract is covered in [Building an Effective Managed IT Services RFP for Public Entities](#).

When is an MSP not the right answer?

Short answer: When the entity would not supervise the provider, when a strong in-house team needs support and not a handover, or when the main exposure is something an IT partner does not cover.

- **A capable in-house team may want co-managed IT.** The provider takes defined work, such as after-hours monitoring or backup testing, and your staff keeps control.
- **Accountability does not transfer.** Leadership still owns decisions, budgets, and public trust. If no one will review the provider's reports, do not outsource.
- **A provider is itself a vendor with privileged access.** A cyberattack on a Mississippi hosting company in October 2026, described on [our public sector page](#), shows how a vendor can be the point of failure. Ask for the provider's SOC 2 report and read its period, scope, exceptions, and auditor. Ask how its own access to your systems is controlled and logged, and what the exit terms are.

- **Utilities and operational technology need specialists.** An IT partner should say so and work with that specialist, not pretend to cover it.
- **Nothing is a guarantee.** Be wary of any provider, including us, that promises an incident will not happen.

How should a public entity decide?

Short answer: Define outcomes, ask for evidence before you sign, and put reporting and exit terms in the contract.

- Who has administrator access to our systems, how is it logged, and how is it removed when someone leaves?
- How do you test backups, and can you show a recent restore with the time it took?
- How will you handle an incident at 2 a.m. on a Saturday: who calls whom, and how fast?
- What are the exit terms, and can we speak with a reference in a similar environment?

The full list of requirements, service levels, and evaluation criteria is in [Building an Effective Managed IT Services RFP for Public Entities](#). Your procurement office decides how the contract is bought.

Why AdvancedBITS?

Short answer: We pair managed IT experience with reporting you can read, and we are plain about our limits.

The points below are company-reported, so verify them the way you would any vendors.

- **20+ years** of managed services experience.
- **Independently audited** to the SOC 2 Type II standard. Read the report, do not take our word for it.
- **Managed or co-managed**, so your in-house staff keeps control if you want it.
- **Documented.** Diagrams, inventories, and recovery procedures are kept current, so knowledge does not depend on one person.
- **Plain limits.** We do not guarantee outcomes, we do not give legal or compliance advice, and we do not replace your leadership or procurement office.

Frequently Asked Questions

Should a public entity hire a managed services provider?

Often yes, when technology depends on one person, projects stay unfinished, cybersecurity needs outgrow staff, or costs are unpredictable. A capable in-house team may prefer co-managed IT instead. Either way, choose a provider that documents its work, reports regularly, and can show evidence, and keep leadership oversight in place.

What does a managed services provider do for a city or county?

A managed services provider (MSP) runs, secures, backs up, and documents a public entity's technology under a written agreement, either fully or alongside in-house staff. It typically supplies help desk support, security monitoring, Microsoft 365 administration, backup and recovery testing, planning, and regular reports.

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

With fully managed IT, the provider runs the entity's technology day to day. With co-managed IT, the provider works alongside in-house staff and takes on defined work, such as after-hours monitoring, patching, backup testing, or reporting, while the internal team keeps control. Entities choose the model that fits their staff and risk.

Will an MSP make a public entity secure?

An MSP can add monitoring, patching, multifactor authentication, tested backups, and an incident plan, which reduce risk. No provider can guarantee that an incident will never occur, and organizations with strong controls have still been compromised. Ask for evidence of what is in place and how it is tested.

How does an MSP reduce dependence on one IT person?

An MSP spreads knowledge across a team and keeps documentation current, including diagrams, inventories, passwords policy, and recovery steps. The test is simple: could someone else run the environment from the documents if your administrator were unavailable tomorrow? Ask the provider to demonstrate it.

How should a public entity compare MSP cost with hiring staff?

Compare the full cost of coverage, not only salaries: after-hours response, backup staff, security tools, training, and projects that never get done. Ask each provider what the monthly fee includes and excludes, and how projects are priced. The answer depends on your size and starting point, so no single figure applies.

Is there evidence that MSPs improve outcomes for local governments?

We did not find a published study that measures local governments before and after hiring an MSP. The evidence concerns why entities struggle and which controls reduce risk. The practical test is your own baseline and a re-measurement at 90 days, using measures such as restore time, multifactor authentication coverage, and patch age.

When is an MSP not the right choice?

An MSP is not the right choice when no one will supervise the provider, when a strong in-house team needs support rather than a handover, or when the main exposure is operational technology that needs a specialist. Be cautious of any provider that promises to prevent incidents.

Does AdvancedBITS provide legal advice?

No. AdvancedBITS provides technology, security, and planning services. Your counsel and procurement office decide which laws, standards, and contract terms apply to your entity, including privacy, public records, and procurement requirements.

Closing perspective

Hiring a managed services provider is a reasonable choice for many public entities, but it moves the work and not the responsibility. The right partner documents, reports, tests recovery, and shows evidence. Test the claims, and measure the difference against your own baseline.

See where your entity stands before you decide

A specialist will review your technology, security, backups, and reporting and show you where a managed partner would help, and where it would not. No cost, no obligation.

Schedule Your Complimentary Public Sector Technology Assessment

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

Sources

Incident details come from the entity's own statements where available, otherwise from news coverage. The Sophos survey is vendor commissioned. The two tables of signs and managed-partner benefits are AdvancedBITS reasoning.

- Research: [Waltz and Gasco-Hernandez, HICSS 2025](#); [Sophos State of Ransomware 2025](#) and [whitepaper](#); [Public Technology Institute 2024 survey](#)
- Cases: [City of Saint Paul incident report](#); [BleepingComputer on St. Paul](#); [NBC Bay Area on Foster City](#); [Smart Cities Dive on DCHA and housing authorities](#); [WAPT on Vicksburg](#); [The Vicksburg Post](#)
- Guidance: [NIST Cybersecurity Framework](#); [CISA SCuBA project](#); [MS-ISAC](#)
- AdvancedBITS: [Managed IT and Cybersecurity for Public Entities](#); [Building an Effective Managed IT Services RFP for Public Entities](#); [Public Sector IT Case Study: Employee Onboarding and Security at a Public Agency](#)

Secure. Accountable. Service-Focused. | sales@advancedbits.com | www.advancedbits.com | 561-300-3015