INTERMIXIT

FREE REPORT

No fluff. No tech-speak. Just facts every Municipality should know.

Municipalities At Risk: The IT Budgeting Gaps That Make You a Sitting Duck for Hackers

Nearly 70% of ransomware attacks on U.S. local governments succeed — and many victims admit they were operating with outdated systems, weak security, and inadequate IT budgets.

INTERMIXIT

Municipalities at Risk: The IT Budgeting Gaps That Make You a Sitting Duck for Hackers

Nearly 70% of ransomware attacks on U.S. local governments succeed — and many victims admit they were operating with outdated systems, weak security, and inadequate IT budgets. The result is more than just a technology problem; it's a disruption of public services, loss of citizen trust, and in some cases, millions of taxpayer dollars spent on recovery.

For municipalities, reliable technology is the backbone of daily operations. From processing permits and managing payroll to providing emergency response coordination and protecting sensitive citizen data, your systems must work seamlessly and securely. Yet too often, IT budgets are built around "keeping the lights on" rather than proactively defending against cyber threats.

Hackers know this. They target municipalities precisely because many operate with tight budgets, limited staff, and outdated infrastructure, making them easier to breach and slower to recover. The cost of underbudgeting for IT is not just measured in ransom payments; it includes operational downtime, legal liability, reputational damage, and the erosion of public confidence.

This guide outlines the most common IT budgeting gaps we see in municipalities, the risks they create, and the steps you can take to secure your systems, protect your data, and safeguard public services. Whether your IT is managed internally, outsourced, or a combination of both, closing these gaps now will help ensure your municipality is prepared for the next cyber threat.

Gap #1: Treating IT as a Cost Center Instead of a Critical Service

In many municipalities, IT is viewed as a line-item expense rather than an essential public service. This mindset leads to the bare minimum being allocated for technology, enough to keep basic systems running, but not enough to modernize, secure, and future-proof the infrastructure.

Without the right investment, municipalities rely on outdated hardware and unsupported software, both of which are prime targets for cybercriminals. Even worse, insufficient resources often mean no dedicated IT security role, leaving network monitoring and incident response on the back burner.

What to Check

- Is your IT budget aligned with the critical nature of public services and the sensitivity of the data you manage?
- Have you benchmarked your IT spending against municipalities of similar size and complexity?
- Does your budget include funds for proactive security measures, not just break-fix support?

Gap #2: No Dedicated Cybersecurity Funding

Many municipalities lump cybersecurity costs into general IT spending, which means they often get deprioritized when budgets tighten. Without dedicated funding, essential safeguards, like advanced threat detection, employee security training, and 24/7 monitoring, are the first to be cut or postponed.

This leaves systems vulnerable to ransomware, phishing attacks, and insider threats, all of which can shut down essential services and expose sensitive citizen records.

What to Check

- Does your budget have a separate line item for cybersecurity, with clearly defined goals and metrics?
- Are you funding both the technology and the training needed to defend against attacks?
- Do you have a plan for scaling security investment as threats evolve?

Gap #3: Underestimating the Cost of Downtime

When hackers take down a municipal network, the impact extends far beyond IT. Emergency response coordination slows, permit processing halts, payroll systems stop, and public-facing services go dark. The cost of downtime can dwarf the cost of proper prevention.

Yet many municipalities fail to factor downtime risk into their IT budgets, leaving them without the resources for rapid recovery solutions, redundant systems, or disaster recovery testing.

What to Check

- Have you calculated the cost of one day or even one hour of system downtime for your municipality?
- Does your budget include funding for backup systems and quick recovery options?
- Are you regularly testing your disaster recovery plan to ensure it works under real-world conditions?

Gap #4: Delaying Hardware and Software Upgrades

Budget constraints often lead municipalities to “stretch” hardware and software far beyond their recommended lifecycle. While this may save money in the short term, it creates significant security and compatibility risks. Unsupported systems don’t receive security patches, making them an open door for attackers.

Additionally, outdated systems often slow operations, frustrate staff, and limit your ability to adopt more efficient solutions.

What to Check

- Do you have a documented hardware and software refresh cycle in your budget?
- Are you factoring in the total cost of ownership, including productivity loss from outdated systems?
- Are all systems currently supported with security patches and updates?

Gap #5: Ignoring Employee Cybersecurity Training

Your employees are your first line of defense against cyber threats and also your greatest risk if they are not trained properly. Without regular, practical training, staff may fall for phishing emails, mishandle sensitive data, or fail to follow security protocols.

Yet in many municipalities, there is no budget allocation for ongoing cybersecurity training, leaving employees unprepared to spot and stop threats.

What to Check

- Does your budget include funding for regular security awareness training?
- Are phishing simulations conducted to test staff readiness?
- Is security training customized for different municipal roles and responsibilities?

Gap #6: Overlooking Third-Party Risk

Municipalities rely on numerous vendors and contractors, from software providers to utility partners. If these third parties have access to your network and systems, their security weaknesses become your risk.

Without budgeted resources for vetting, monitoring, and managing vendor access, municipalities are blindsided by breaches that originate from trusted partners.

What to Check

- Do you have a process and budget for assessing vendor cybersecurity practices?

👉 Next Step: Schedule your 15-Minute IT Budget Check before your next budget is finalized. We’ll show you exactly where your municipality stands — and what gaps may be putting your residents, staff, and reputation at risk. www.intermixit.com/ITbudgetcheck

- Are vendor connections segmented from your core network?
- Is vendor access reviewed and revoked promptly when no longer needed?

Gap #7: No Incident Response and Recovery Funding

Even with strong defenses, no municipality is immune to cyber incidents. The difference between a minor disruption and a major crisis often comes down to how quickly you respond.

If your budget doesn't allocate funds for incident response services, forensic investigation, and post-incident recovery, you may be left scrambling for resources in the middle of an emergency.

What to Check

- Does your budget include funds for an external incident response team?
- Are recovery timelines defined, tested, and achievable with your current resources?
- Have you budgeted for the potential legal and PR costs of a cyber incident?

Why These Gaps Cannot Be Ignored

- 70% of ransomware attacks on local governments succeed due to outdated systems and weak defenses.
- The average ransom paid by U.S. municipalities in 2024 exceeded $900,000, not including recovery costs.
- 93% of municipalities that suffer extended downtime experience significant public backlash and loss of trust.
- Downtime costs for local governments can exceed $50,000 per day in lost productivity and service disruptions.

These numbers aren't scare tactics, they reflect the real and rising costs of underbudgeting for IT and cybersecurity. Closing these gaps protects not just your systems, but the trust of your citizens and the continuity of critical public services.

You Have Seen These Gaps – Now What?

If even one of these budgeting gaps exists in your municipality, you could be one cyber incident away from costly downtime, public criticism, and long-term reputational harm. The first step is to assess where you stand today and create a budget that reflects the true cost of protecting your systems and services.

Our Network Assessment will give you a detailed, actionable report on your current environment, pinpointing the vulnerabilities that could be exploited and exactly what it will take to fix them within your budget.

👉 Next Step: Schedule your 15-Minute IT Budget Check before your next budget is finalized. We'll show you exactly where your municipality stands — and what gaps may be putting your residents, staff, and reputation at risk. www.intermixit.com/ITbudgetcheck

How to Get Started with IntermixIT

- **Book Your 15-Minute Introduction Call – www.intermixit.com/ITbudgetcheck**
  A focused conversation to understand your current IT setup, budgeting challenges, and where security risks could leave your municipality exposed.
- **Get Your Municipality-Focused Cybersecurity Assessment**
  We review your systems through the lens of local government operations — covering public safety systems, citizen data, remote access, backups, and vendor risk.
- **Review Your Results and Explore Your Options**
  We'll walk you through your results, answer your questions, and give you a clear plan to close your budgeting gaps and strengthen your defenses.

Success Story: Lower Swatara Township Strengthens Cybersecurity and Improves IT Reliability with IntermixIT

Lower Swatara Township recognized that their growing reliance on technology to deliver public services also increased their exposure to cyber threats. Outdated systems, limited in-house resources, and increasing security risks made it clear they needed a partner who understood municipal operations and could proactively protect sensitive data.

IntermixIT stepped in with a customized IT strategy to address Lower Swatara Township's specific needs. Here's how they made an impact:

The results:

- **24/7 IT Support:** Ensuring no downtime, especially for critical departments like the police force.
- **Advanced Cybersecurity Measures:** Implementing robust security protocols, including network backup and recovery plans to safeguard against future cyberattacks.
- **Proactive IT Management:** Quarterly reviews with Zachary to discuss priorities, budgeting, and project updates, ensuring technology aligns with your goals.
- **Employee Cybersecurity Training:** Providing ongoing phishing exercises and training to keep staff informed and vigilant.

Today, Lower Swatara Township operates with a technology foundation that supports efficient service delivery, minimizes downtime, and defends against the growing wave of cyber threats targeting municipalities.

Read the full case study here: Lower Swatara Township Success Story

👉 Next Step: Schedule your 15-Minute IT Budget Check before your next budget is finalized.
We'll show you exactly where your municipality stands — and what gaps may be putting your residents, staff, and reputation at risk. www.intermixit.com/ITbudgetcheck