NYSAC
NEW YORK STATE
ASSOCIATION OF COUNTIES

IT Task Force Report

Working Draft

Technology Issues Facing Counties

JANUARY 2024

HON DANIEL P MCCOY
NYSAC President

STEPHEN J. ACQUARIO
Executive Director

PAUL LUTWAK
NYSAC IT Task Force Chair

United Voice of NY Counties

📍 515 Broadway, Suite 402
Albany, NY 12207

@ www.nysac.org

☎ 518-465-1473

Introduction

In 2021, the Board of Directors for the New York State Association of Counties created the NYSAC IT Task Force to serve as an advisory group to discuss major information technology (IT) and data issues that impact the operations and governance of counties.

The mission of the IT Taskforce is to work cooperatively to provide advice, strategic direction, collaboration, and insights for the safe, secure, and effective use of information technology in counties (and all governments) across New York State. Some of the members of the Task Force are from county IT departments, others represent cross-functional roles in your counties. All have an interest in and a concern about the role that information technology and systems play in the business of county government. IT is the backbone of the back-office operations of every county department across the state.

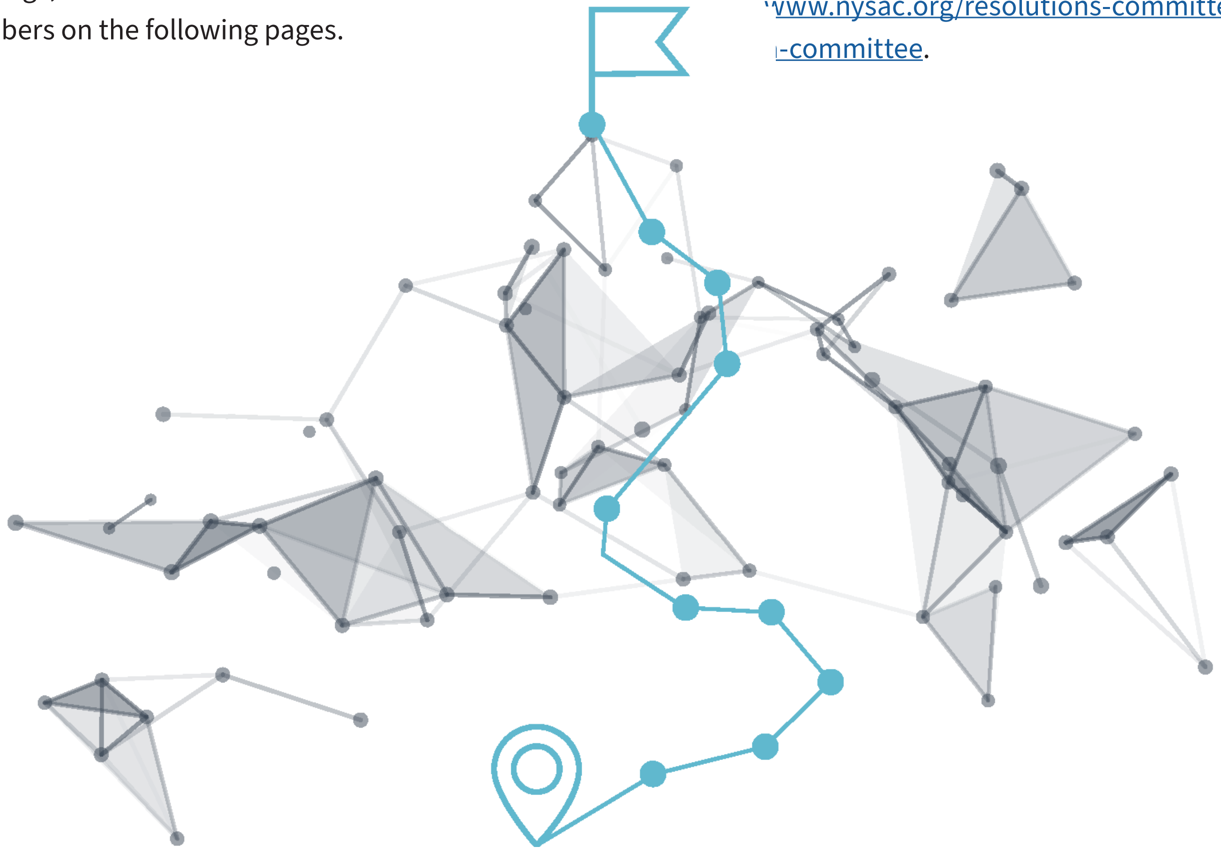
This summer and fall, the IT Task Force developed a working list of the top technology-focused issues, concerns, and opportunities facing county governments across the state. These items have been prioritized and categorized under the following headings, with more details from Task Force members on the following pages.

As Task Force members discussed these items, there were many connections that uncovered the interrelated and complex nature of building a strong IT infrastructure of hardware, software, and staff.

- Workforce
- Cybersecurity
- IT Governance and Departmental Structure
- Intergovernmental Service Sharing
- Funding and Grants
- Transitioning to .Gov

This Task Force report is designed to raise awareness and understanding of the technology expertise, resources, and needs that drive the business of government at the county level in New York. Where we have recommendations, they are listed at the end of each section.

If you or a member of your county is interested in joining the NYSAC IT Task Force, please fill out and submit a nomination form at https://www.nysac.org/resolutions-committees/join-a-committee.



Workforce

Recruiting and retaining qualified staff at the local government level has become very difficult, particularly in areas where the private sector offers more competitive salaries, benefit packages, and work-from-home options. Finding strong IT professionals is critical to our IT infrastructure development, cybersecurity capabilities, and effective IT service delivery. While counties across the nation are having difficulty recruiting and retaining qualified workers, IT departments may be one of the most challenging teams to put together.

“The challenges range from competitive pay to benefits including flexible schedules and remote work, as well as training and career advancement opportunities,” according to the National Association of Counties (NACo). In New York State, archaic and outdated civil service laws make it even harder to bring in new qualified staff. Civil service requires us to hire for titles that no longer align with the needed IT positions, and the exams don’t match today’s qualifications.

Every county has different needs and resources, but they also have different policies and procedures when it comes to identifying and justifying new positions and the hiring process.

Under our current government setup, there is no provision for an agency or department to hire a replacement worker to be trained when a person leaves their role/position. The outgoing person is not given the opportunity to transfer their institutional knowledge to the new employee who is taking over their role. It could take an immense amount of time for the new person to acquire the same knowledge and expertise. Due to the constraints of civil service, agencies and department may not be able to hire anyone for months or years. Forcing a new employee to solely learn on the job has dire consequences such as:

1. Making mistakes that could result in low morale and low employee retention,
2. Financial losses to the department or agency,
3. Project delays,
4. The ripple effect of other staff trying to help fill the knowledge gap and forcing delays in their own work, and
5. Delayed or incorrect service delivery to taxpayers.

Task Force Comments

“Many counties have smaller IT departments, and our wage scale doesn’t work to compete with private sector technology positions.”

“Once hired, our employees need training and skills development to meet the ever-evolving technology innovations effecting businesses and governments, and the residents we are here to serve.”

“We need to address and plan for comprehensive training and skills development for our IT staff.”

“The one thing I think everyone could do is encourage internships. If all county IT departments could set up two internships for college IT students, we could grow our own NY workforce. The cost isn’t that high. Maybe a state grant for internships? I currently have two full time staff members that were interns here. I currently have an intern that started as a freshman in college and will have 4 years of internship. I may not have a spot for him when he graduates, but I’m positive he will be an asset for any county.”

Recommendations

- The state needs to review and reform civil service requirements to make it much easier for local governments to attract and retain talented IT professionals.
- All IT leadership positions should be salaried, non-union positions.
- Standardizing titles, functions, and job descriptions of county IT professionals would be helpful, however challenging.
- Department or agency heads should be allowed to hire a new person while the outgoing employee is still in their position. Position overlap allows two individuals to occupy the same position for a limited period of time so that the outgoing employee can train the incoming worker.

Cybersecurity

***"We need to harden our cybersecurity without specialized staff and on a limited budget."* – IT Task Force Member**

Hardening cybersecurity involves the systematic reinforcement of digital defenses to enhance the resilience of information systems and data against cyber threats. This process encompasses a comprehensive set of measures, including implementing robust access controls, regularly updating and patching software vulnerabilities, configuring network and system components with stringent security settings, employing strong encryption methods, conducting regular security audits and assessments, fostering a security-aware organizational culture, and swiftly responding to and recovering from security incidents. By fortifying digital infrastructure through these multifaceted strategies, organizations can significantly reduce the potential attack surface and mitigate the impact of cyberattacks, ensuring greater protection of sensitive information and maintaining the integrity, availability, and confidentiality of their digital assets.

According to NACo's Technology Advisory Council, "It is vital that county leaders communicate with the county IT leadership or the outsourced IT support concerning the important cyber posture of the county… While it is the responsibility of IT to implement many of the day-to-day cyber best practices and for other department leaders to provide the business requirements, it is your responsibility to understand the impacts that these cyber efforts have in relation to resources, budget, legal requirements, and ultimately the safety of the county data assets."

Local governments face several critical issues related to system backups. These include insufficient backup strategies, limited resources and infrastructure, compliance and data retention requirements, budgetary constraints, backup security concerns, and the need for testing and verification. These challenges can lead to data loss, prolonged downtime, and difficulties in recovering essential services during disasters or system failures. We are finding that we do not have the staffing to keep up with increasing demands related to backup systems.

Recommendation

- State-sponsored backup solution that would help local governments mitigate the critical issues and challenges that they face.

The New York Joint Security Operations Center (JSOC)

Launched in February of 2022 as first-of-its-kind hub for data sharing and cyber coordination across the state, the JSOC now includes nearly every county in New York State.

High Availability and Disaster Recovery

High Availability (HA) and Disaster Recovery (DR) are critical components of a comprehensive IT strategy aimed at ensuring the continuous operation and resilience of systems, applications, and data. High Availability involves designing and implementing redundant and fault-tolerant architectures to minimize downtime and provide seamless access to services in the event of hardware or software failures. Disaster Recovery, on the other hand, focuses on planning and implementing strategies to recover and restore IT operations after major disruptions such as natural disasters, cyberattacks, or system failures. Together, HA and DR solutions aim to reduce service interruptions, minimize data loss, and enable rapid recovery, thereby safeguarding business continuity and minimizing the impact of unforeseen events on organizational operations.

Data Classification

Data classification is the process of categorizing and labeling data based on its sensitivity, value, and regulatory requirements. By assigning different levels of classification, such as "confidential," "public," or "internal use only," organizations can effectively manage and protect their data according to its importance and potential impact if compromised.

This classification helps determine appropriate access controls, encryption measures, retention policies, and other security measures, ensuring that data is handled and stored in alignment with regulatory compliance and the organization's security policies.

Continuity of Operations

A continuity of operations (COOP) plan is crucial for a county government to ensure our ability to maintain essential functions and services during unexpected disruptions or emergencies. A well-developed COOP plan anticipates potential threats, ranging from natural disasters to pandemics or cybersecurity breaches, and outlines clear procedures to mitigate their impact. By establishing alternate facilities, communication protocols, and contingency measures, a county government can ensure the seamless delivery of essential services even in the face of adversity. This proactive approach not only safeguards the well-being of the community but also promotes public confidence in the government's ability to manage crises effectively. The county administration should be directly involved in the overall COOP and each department should have one as well.

Table Top Exercises

The most valuable thing we can do for cybersecurity is education. One of the best tools for educating our managerial staff are tabletop exercises. The online simulations can be valuable, but nothing replaces an in-person tabletop exercise with the whole incident response team. The State's Division of Homeland Security and Emergency Services (DHSES) conducts excellent tabletops exercises, however, to be fully efficient, counties need to be conducting these exercises at least once a year. DHSES, at this time, is not staffed to be able to do this for all counties once a year.

Recommendation for Expanding Tabletop Exercises

We need either the State Office of General Services (OGS) or a large county to issue an RFP for in-person tabletop exercises for all counties. Hopefully by stating in the RFP that all counties would be part of this, the costs will be reasonable. That way, maybe Homeland security grants could be used. Additionally, maybe until DHSES is fully staffed, State money that is being allocated to other departments could be earmarked for this (for example, federal and or state funds that are directed to BOE could be used for a BOE specific tabletop exercise.)

Election Specific Security

IT must be fully partnered with the BOE counterparts in operations, physical and cyber security, and electronic and paper flow. Understanding each other's responsibilities is key to success. We must approach this issue based on our current threat landscape regardless of the political background. The confusion between the facts and truth that naturally comes with political campaigning is simply part of the politics we need to tune out while we focus on the protection of our election process.

Understanding the Election Process Chain

This effort is to ensure the I.T. staff understands the obligations of the BOE staff and vice versa.

Identifying our assets

To protect, we need to know the components at risk.

Identifying the threats

Knowing the past and present threat landscape is critical for a successful outcome. It is important to understand that not all threats are 'cyber' related, such as the intent to cause distrust in the election process.

Playing defense

This is the core of our efforts. The largest disadvantage in this field is the amount of information that is publicly available. The type of equipment used is publicly available that can assist with targeted attacks. Most of the voter information is also publicly available, including name, mailing address, physical address, sex, date of birth, email address, phone numbers, last time voted, last method voted, voting district, local voter ID, NYS voter ID, and voting district.

Proving your efforts

The election is over. The certified results are on their way to Albany. This is usually where everyone concludes we are done. This is the time when we must be prepared to be put under the legal microscope following each election.

IT Governance and Departmental Structure

Like many of the items that made the Task Force's list of issues, these items address two distinctly different areas, but have a common thread. IT Governance addresses the policies that govern a county's deployment, procurement, and use of technology; while the departmental structure focuses on how the IT team is organized and conducts its critical day-to-day work.

The common thread is this: IT governance refers to the framework and practices that organizations adopt to effectively manage and align their information technology (IT) strategies with overall business goals and objectives.

It involves establishing decision-making processes, structures, and controls to ensure that IT investments, resources, and initiatives are in line with the organization's strategic direction and risk appetite.

IT governance encompasses areas such as defining roles and responsibilities, setting up accountability mechanisms, managing IT-related risks, ensuring compliance with regulatory requirements, and optimizing IT performance and value delivery.

By implementing robust IT governance practices, organizations can enhance transparency, accountability, and decision-making in their IT operations, leading to improved efficiency, risk management, and alignment between technology and business outcomes.

There needs to be better relationships between all departments and IT. One of the goals of the NYSAC IT Task Force, and this report, is to open dialogue between all functions and departments in a county.

This open communication will foster greater trust and more collaboration. The role of IT is to support the back office of all county operations. When we are talking and working together, we all can do a better job serving residents.

Recommendations

All county IT purchases must flow through IT. We need to know what is being purchased. We need to vet all software purchases prior to the purchase. We need to be able to say no to some purchases. Vetting also can prevent multiple software packages that accomplish the same thing. This will save on costs, both time and money. All purchasing contracts must have a cyber-security insurance clause that is commensurate with the risk that that software could pose in case of a breach.

Task Force Comments

"Even though our county's multiple IT department were consolidated in 2019, there are still a couple of departments with IT tech positions. And, in general, elected officials and department heads would like to have their own IT technicians."

"Given recent experiences impacting counties, the complexity of contemporary IT and the threat environment we face, the existence of separate IT teams in any county is untenable and a bad practice. Consolidation of IT authority under a director or CIO needs to be done at the statutory level in all municipalities."

Intergovernmental Service Sharing

Shared Services

County IT departments are often asked what they can do to support local cities, towns and villages who are also understaffed in IT. Many municipalities have outsourced their IT support and are either not happy with the services or find it expensive to maintain. Rather than focus on the support of a desktop computer the state should consider services that could be consolidated under the county umbrella that might ease some burden on the CTVs such as expansion of the Crowdstrike initiative, adding KnowB4 phishing training for all as an offering, and offering SIEM services.

More and more county and local government processes need systems sharing between levels of government. For example, the state's discovery changes involved requirements for the police and district attorneys to share data. There needs to be time and resources spent on discussing the best ways to develop and implement retention, backup, and storage policies and procedures. This data takes a lot of storage."

"In Madison County, we provide shared IT services to 11 towns/villages. This will never be a money making venture for the counties. It isn't meant to be. The value added to the towns and villages is huge. These partnerships also pay off as it opens up another mode of communication between the county and towns and it brings other county initiatives closer to the towns and villages."

Funding and County Grants

IT is the backbone of almost every county department, operating the business systems—computers, databases, software, and hardware—that support the functions of any given local government program or service. Even so, when a county department receives a state or federal grant there are often no funds allocated to the IT department to support the new systems needed to fulfill the grant requirements. IT Directors, CIOs and their staff members have indicated that being part of the grant process and receiving a percentage of the grant would be helpful in achieving the overall goals of the effort.

Thought needs to be given to what happens with the equipment after the grant expires, and that can happens through conversations or a formal process for determining how systems get paid for and serviced. This should happen before grant funding is expended, not after.

Recommendation

- IT departments need to be included in the grant process – for both federal and state grants – and receive a portion of funds whenever there is an IT component to fulfilling the grant requirements.

Transitioning to Dot Gov

Under current law enacted in 2022, counties in New York State need to transition to dot gov by August 2024.

Transitioning to a ".gov" domain involves the process of shifting an organization's online presence from a generic top-level domain (TLD) like ".com" or ".org" to the official ".gov" domain, which is reserved for U.S. government entities. This transition signifies an authoritative and government-affiliated digital identity, enhancing trust and credibility for users seeking official government information and services. The migration typically involves technical adjustments such as domain registration, website content migration, and ensuring compliance with government standards for security, accessibility, and information accuracy. By adopting the ".gov" domain, organizations can better align with their governmental status, prioritize user confidence, and reinforce their commitment to providing accurate and reliable information and services to the public.

"The state needs to determine if this will be pushed to all municipalities or not. A timeline is needed. This will tie into the shared services that many of us deliver to cities, towns, and villages.

Additional Issues Under Consideration by the NYSAC IT Task Force

1. While the items addressed previously in this report were identified as some of the most critical IT issues facing counties, the following concerns were also raised and will be considered by the members of the Task Force going forward.
2. Artificial or Augmented Intelligence (AI).
3. New Initiatives (EMS, 9-11, others).
4. Data Driven Decisions.
5. Accessibility in communities across the county. Fiber runs to unconnected (underserved) communities.
6. Contracts, vendor management, and cybersecurity insurance.
7. EMS technologies. Outfitting vehicles and people.
8. Virtualization.
9. Improving the User Experience.

NYSAC IT Task Force Members

Laura	Baker	Chief Information Officer	Schenectady County
Thomas	Bunn	CIO	Cayuga County
Michael	Burns	Director Information Technology	Genesee County
Chris	Caccia	Director of Technology	Schuyler County
Daniel	Castricone	Risk Manager	Orange County
Robert	Corpora	County Administrator	Cortland County
Alicia	D'Amico	Dep Comm., Dept. of General Services	Orange County
Lorne	Green	Chief Information Officer	Sullivan County
Timothy	Groth	Information Technology Director	Yates County
Scott	Haverly	I.T. Director	Schoharie County
Elaine	Jardine	County Planning Director	Tioga County
Rick	Johnson	I.T. Director	St. Lawrence
Chad	Klotzbach	County Legislator	Genesee County
Paul	Lutwak	Director of Technology	Madison County
Chirstine	O'Herron	Deputy Commissioner - DSS	Chemung County
Michael	Ponticiello	Deputy County Executive for Physical Services	Broome County
Greg	Powlin	Director of Central Services	Oswego County

NYSAC

Since 1925

UNITED

The United Voice of New York's Counties

New York State Association of Counties

515 Broadway, Suite 402
Albany, NY 12207

@ www.nysac.org

☎ 518-465-1473