TAYLORED Advisor

HOW GOVERNMENT FACILITIES CAN IMPROVE TECHNOLOGICAL EFFICIENCY

TABLE of CONTENTS

MODERN GOVERNMENTS DEPEND ON RELIABLE TECHNOLOGY

WELCOME TO THE ERA OF DIGITAL GOVERNMENT. From the DMV to EMS, digital transformation has the potential to completely alter how — and how efficiently — government services are delivered to constituents.

Today, even the smallest local governments are allowing citizens to apply for building permits online or integrating law enforcement software to manage police investigations. New online portals allow users to pay parking fines, schedule electric hookups and manage property taxes — all without leaving their homes. Some governments have even moved critical services like 311, emergency dispatch and vital records online, leveraging cloud storage, mobile platforms and even AI chatbots to ensure the efficiency, accuracy and accessibility of various government services.

Yet, with more online services comes more risk: When lives are at stake, downtime is not an option. Leveraging the cloud means storing more data online — and potentially risking the exposure or theft of sensitive information. Slow or ineffective technology can leave citizens and government employees alike frustrated, potentially negating the benefits of moving online.

In a 2017 survey from Gartner, government CIOs said they expected to spend over a fifth of their budget on digital initiatives.

It's not enough just to leverage technology. New systems and services must be integrated in an environment of robust digital infrastructure, streamlined workflows and strong cybersecurity protections. In other words, technology needs to be not only effective, but efficient.

WHEN UPTIME IS A MATTER OF LIFE AND DEATH

For government organizations, IT systems may be the link between citizens and lifesaving services. In an emergency situation, every second counts, which is why uptime is critical. Immediate response and communication is crucial for saving lives.

First responders, and dispatch systems for police, fire and sheriff, all rely on sophisticated technology to protect lives and property. They need more than just fast recovery after an emergency or failure. When lives are at stake, they need to be able to detect and prevent failures before they occur.

Critical Services Going Digital

Here are four ways governments are leveraging technology for vital services.

Dispatch services: Sophisticated tools allow call takers to geographically locate citizens in need of assistance and dispatch law enforcement or fire services to the scene immediately.

Disaster response: Moving services to the cloud means that first responders can continue providing services even if on-site servers are interrupted due to a major disaster or other interruption.

Crime prevention and investigation: Sophisticated IP cameras are giving law enforcement a clearer picture into the crime in their jurisdiction.

Communications: Mobile tools allow police and emergency responders to react to critical threats swiftly and succinctly.

OTHER GOVERNMENT SERVICES ARE GETTING DIGITAL TREATMENT

The potential applications of digital transformation throughout government are many and varied. Here are a few of the most common uses we've seen.

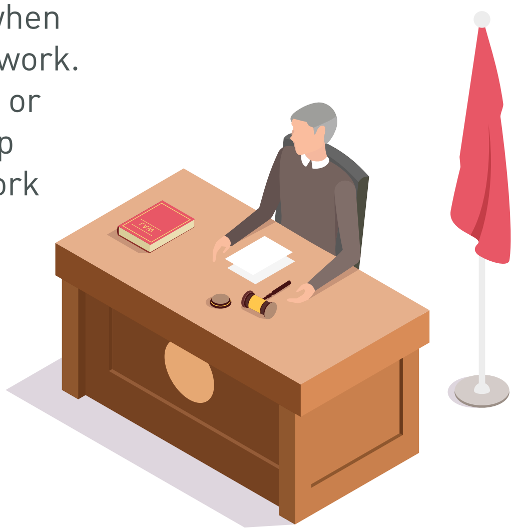
Legal and court systems: Governments are leveraging powerful new technologies to help constituents schedule court dates and resolve civil disputes online. On the back end, cloud storage and software help court employees manage the administrative burden, freeing up time for more useful work.

Public works and road crews: New tools help these sectors streamline complex and varied projects so that road crews can get jobs completed faster and more efficiently.

Mapping and city planning services: When it comes to GIS services, mapping and city planning, secure and efficient networks mean improved safety and operations.

Public utilities: Regulatory pressures, consumer expectations and expanding complexity of the smart grid infrastructure are all challenges in this sector — but managed services help optimize business processes for government facilities.

With the right technological capabilities, digital innovation can literally transform your government. However, when these services don't work, your government doesn't work. Each government sector — whether municipal, state or federal — relies on secure, efficient networks to keep constituents safe and served. In many cases, a network failure or other critical event can literally mean the difference between life and death.



CHALLENGES TO GOVERNMENT CYBERSECURITY

Uptime isn't the only challenge for digital government. Agencies are increasingly vulnerable to cybersecurity threats — in 2017 alone, 35,277 cyber attacks were reported by US federal agencies. A major breach could throw your government into disarray, costing thousands or even millions of dollars to recover data and mitigate the damage.

However, governments are becoming a favorite target of cybersecurity threat actors. Since governments have access to incredibly sensitive data, such as social security numbers and birth certificates, hackers can use this information as leverage to trick governments into paying exorbitant ransoms — or simply turn around and sell it on the dark web.

Since this information is consistently used in the public sector, it's critical that government agencies secure and recover sensitive information in case of a breach or disaster.

Ransomware — a form of malware that encrypts files until a ransom is paid — is a malicious form of cyber attack that's on the rise for state and local governments. As of October 2019, 140 local governments, police stations and hospitals had suffered ransomware attacks this year.

BUILDING ROBUST IT SYSTEMS ON LIMITED RESOURCES

Another challenge for government IT managers and CIOs comes not from technology and/or potential failures, but from the nature of government itself. Many agencies are tasked with implementing new technologies on tight budgets, with limited resources to support them. There may be challenges or delays obtaining approval for more aggressive initiatives. Even routine updates can be difficult where there isn't enough staff to thoroughly plan and manage these kinds of necessary interruptions.

Here's a sampling of some of the challenges agencies are facing as they shift to a more digital approach to government.

Budgetary Concerns

For some government organizations, funding is a major issue. Federal budgets become tighter every day, which limits IT managers and staff to system upkeep rather than innovative solutions to better protect and optimize the IT infrastructure.

Value and ROI are also important — IT managers need to be able to prove that solutions are cost-effective as well as effective. Because IT staff is responsible for proving a significant ROI for expensive IT systems, it becomes a case of doing more with less.

Initiatives often require board approval or other sign-offs. When government agencies manage their own network, they make contractual commitments for hardware and software. With the release of each new version, more contract revisions are necessary, which means more time waiting on manager approval.

Limited Internal Resources

Especially for smaller agencies with limited staff and other resources, it's easy to get behind on keeping up with innovative IT solutions that are critical for an optimized infrastructure.

Security threats are so sophisticated that it often takes a whole team of experts — not to mention heavy software and hardware investments — just to manage and implement cybersecurity tools. Many government agencies don't have the resources or funding for this specialized expertise.

Most government workers are promoted from within, which means they can lack the specialized experience to combat high-profile security risks.

Planning Maintenance and Upgrades

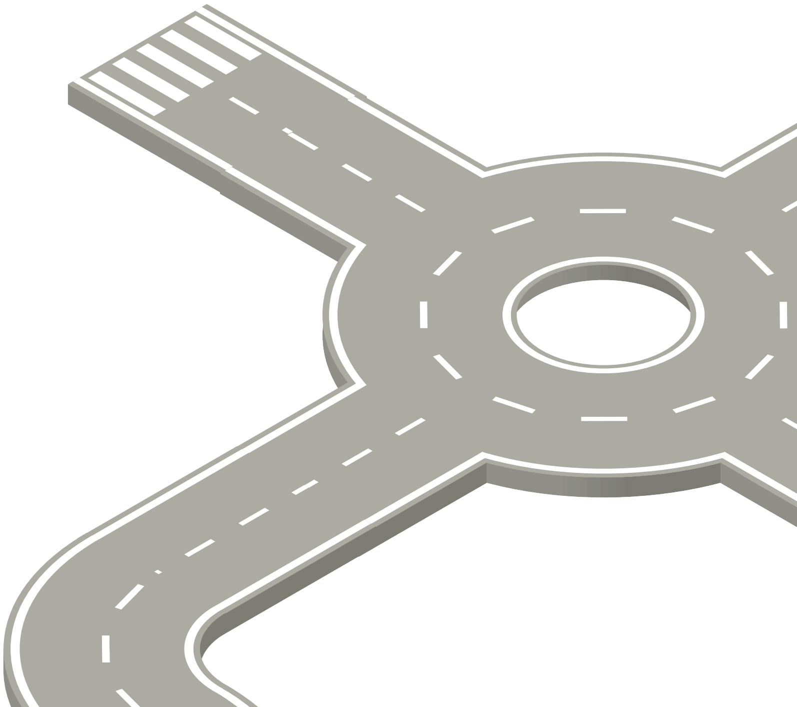
It's critical for government agencies to be able to plan maintenance windows and upgrades in a way that doesn't impact government services. However, a lack of funding or resources makes this difficult, which means that IT networks are vulnerable to system failure, data breach or cyber attack.

THE FUTURE OF GOVERNMENT TECHNLOGY

WHEN WE SAY CITIES ARE GOING DIGITAL, WE MEAN IT. Along with the technologies already in use by many governments today, the promise of new tools like machine learning, analytics, automation and even AI may make tomorrow's government technology virtually unrecognizable to today's.

In the future, governments will face pressure to move more services online and leverage new public safety technologies while at the same time navigating an increasingly sophisticated cybersecurity landscape.

Specifically, here are a few of our predictions for the near future of government IT.



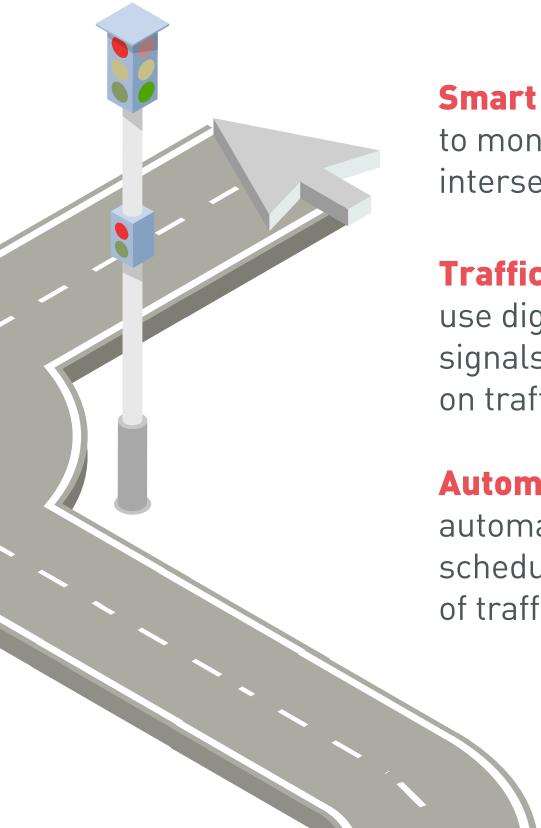
PREDICTION 1: EVEN MORE ONLINE SERVICES

These days, governments that don't offer online portals to tax offices, DMVs and municipal court systems are becoming the exception rather than the rule. People expect 24/7 connectivity so that they can file taxes, register a new company or take care of DMV interactions — without ever having to leave home.

Our first prediction is for more of the same: more services moving online to accommodate citizens who don't want to do things in person. In some cases, governments have launched entire "digital city halls," where constituents can essentially take care of all things government from their laptops. This equates to enormous time and cost savings for agencies, but it also requires complex security and infrastructure planning.

PREDICTION 2: AUTOMATION AND SMART CITIES ARE COMING

The emergence of smart tech and automation is having a massive impact on public safety; more specifically, we expect to see an increasing implementation of the following crime-detection and safety tools.



Smart sensors and cameras: Smart cameras make it possible to monitor government buildings and external campuses and intersections without a huge infrastructural investment.

Traffic lights and traffic signal systems: New technologies use digital transformation to automate and program traffic signals, and can even direct traffic in different ways depending on traffic events.

Automating public transportation systems: Transit automation allows cities to more accurately predict bus schedules and alert and potentially reroute drivers in the event of traffic or other incidents.

Looking even further into the future, the concept of the “smart city” may come to fruition. In this vision, cities will leverage internet of things (IoT) devices such as connected sensors, lights and meters to collect and analyze big data. This, in turn, will be used to improve public utility infrastructure and efficiency, track and monitor streets, and manage public safety.

Cities like San Francisco, Pittsburgh and Boulder have already begun implementing smart infrastructures, such as smart electricity grids, parking systems, transit systems and microgrids for alternative energy. As these technologies become less foreign, easier to implement and less expensive, we expect to see more widespread use of smart systems.

PREDICTION 3: EVER MORE COMPLEX SECURITY CHANGES

Like all entities, government agencies face ever more elaborate and sophisticated cybersecurity threats. Cybercriminals are now able to study the online behavior of users and network activity to design sophisticated social engineering tactics to steal data and assets and threaten organizations.

Government, however, faces unique challenges in the cybersecurity space. Not only do these agencies hold incredibly sensitive information — data that, in the wrong hands, could have disastrous effects — but they’re also typically the target of highly calculated cybersecurity tactics.

Instead of merely trying to steal a few credit card numbers, government threat actors often have much loftier and sinister goals, political or otherwise. They often pursue government data as a full time job and will be more motivated to continue to find ways into government networks and systems.

Because government organizations are a vulnerable target for these attacks, it will become even more critical to be on high alert and routinely implement layered security solutions to defend against all threats, from phishing and social engineering to data breaches and ransomware. Government IT departments will have to stay one step ahead of evolving trends and implement the right tools to protect themselves.

EASY-TO-IMPLEMENT SOLUTIONS

SO HOW CAN YOU LEVERAGE ONLINE SERVICES AND NEW TECHNOLOGIES and protect your government from cybersecurity threats — all while staying within budget and navigating the political challenges inherent to implementing such systems?

It's a tall order, but there are a few simple and cost-effective — and uncontroversial — changes that government agencies and organizations can make to protect their data and streamline the efficiency and usefulness of current online systems.

I

RECOMMENDATION 1: CENTRALIZE YOUR IT

Shifting to a more centralized IT model can help governments monitor and maintain IT systems more effectively. Microsoft offers powerful tools for this very purpose, helping agencies take advantage of more organized and centralized controls. For instance, Windows Admin Center makes it possible to manage Windows servers, Azure cloud instances and Windows machines directly through one platform.

A centralized approach also involves:

Implementing new policies and processes. Robust, tested continuity plans and disaster recovery plans will allow you to respond to critical events in an organized and thoughtful way, and pave a way forward afterward. Implementing user awareness training is a key part of this, as it ensures that all users are on the same page and prepared to spot and respond to a potential threat.

Performing system and technology audits. For some organizations, the first hurdle is simply to understand what systems and technologies are in place, and their age and capabilities. Performing an audit will help you know what assets you need to protect and/or replace.

Ensuring backup and disaster recovery. Managed backups are a critical part of a continuity plan, helping you continue operations remotely even when systems fail.

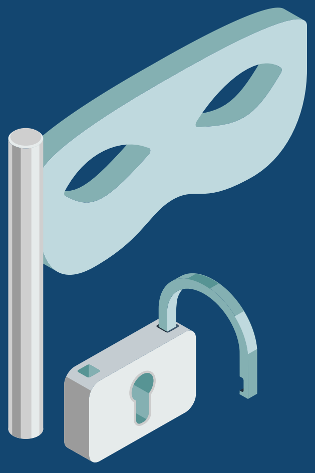
RECOMMENDATION 2: STAY CURRENT WITH SYSTEM UPDATES

Understanding the performance of your IT systems and being able to diagnose problem areas is a must for a healthy network. Planned upgrades also protect you from potentially exploitable software vulnerabilities. We recommend that government organizations:

Evaluate the age of various systems. Older systems are more vulnerable to failure, which makes it critical to evaluate the age of your various IT systems and update or replace accordingly.

Perform software updates. Detect and prevent any software issues before a hacker takes advantage of your IT vulnerabilities. A simple routine update could be what saves your agency from a major cyber attack or data breach.

RECOMMENDATION 3: IMPLEMENT USER AWARENESS TRAINING



From opening phishing emails to failing to use a secure password, there are a host of ways that employees can unintentionally expose your agency to an attack. In fact, users are the greatest threat to government cybersecurity — but user awareness training can help. Expanding their awareness, employees and managers are trained to spot and avoid risks, which protects your business from serious threats and helps you stay compliant.

HOW AN MSP CAN HELP

ENGAGING A MANAGED SERVICES PROVIDER for your government IT systems can help you fill in the gaps in your existing IT management while leveraging cost-effective and more efficient solutions.

CENTRALIZED TOOLS

When it comes to managing your IT tasks, almost nothing helps as much as having centralized tools that streamline your workday and cut down on wasteful downtime. An MSP can help get your agency set up with internal ticketing systems for reporting problems, as well as scheduling and monitoring systems to ensure that you're always one step ahead. An MSP will help you take advantage of existing investments and make the most cost-efficient decisions to save you money and time.

EXPERTISE

Managing an IT system isn't just about performing software updates. From network monitoring to disaster recovery and business technology planning, it takes a host of skill sets to efficiently manage an IT system. And that's where an MSP comes in. With multiple team members on staff to help with server management, backups, cybersecurity and more, you get an experienced and dedicated partner that can recommend the best solutions for every IT need. An MSP can also help you:

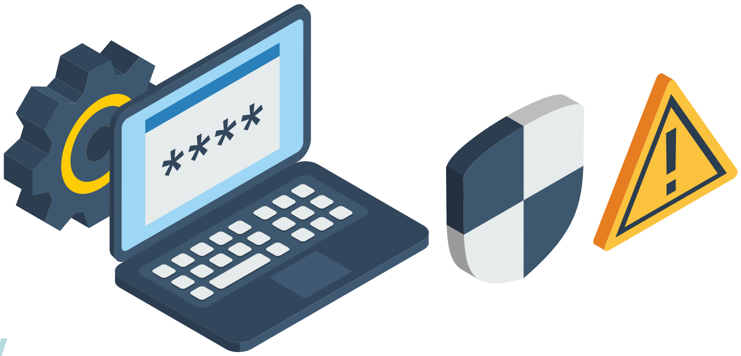
Communicate with vendors. An MSP is your partner in every way — and that includes taking charge of vendors and the needs.

Create policies, such as a disaster recovery plan. Comprehensive disaster recovery and business continuity plans — including onboarding/offboarding policies and security assessments — streamline your workflows and give your agency iron-clad protection against cyber attacks, data loss, network outages and more.

Plan maintenance windows and upgrades. Gain peace of mind knowing that your IT network is secure and optimized enough to handle complex workloads without disruption — day in and day out.

Stay compliant with various standards. An MSP's expertise in network security keeps you and your data safe from threats.

Develop plans to implement and leverage new technologies. From upgrading systems to project planning, budgeting and staying on top of current technologies, an MSP will develop an IT roadmap to ensure your agency's success.



SCALABILITY AND FLEXIBILITY

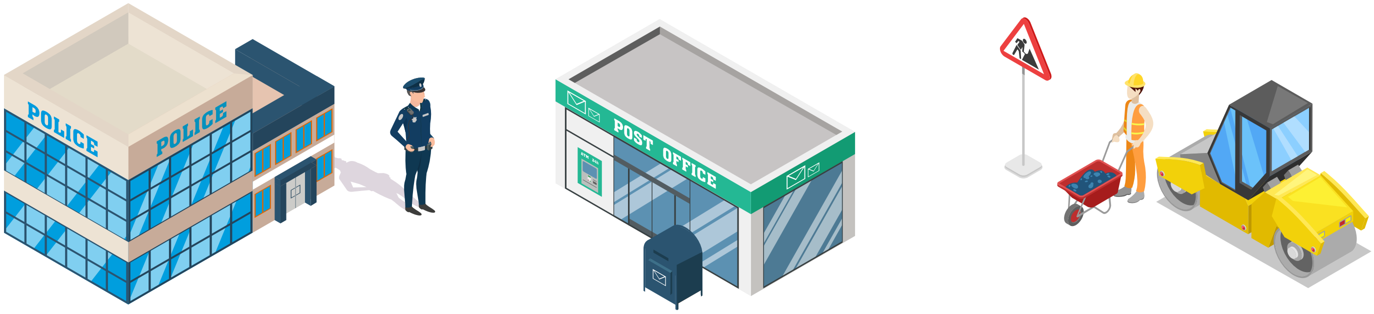
Regardless of whether your agency is poised to grow or your workloads fluctuate, scalability and flexibility are always key in maintaining control and consistency in your agency. By partnering with an MSP, your agency can offload routine tasks, thereby giving your teams the bandwidth to focus on more important work. They'll help scale resources when necessary, and they'll customize solutions to let your team choose how much they want to manage internally versus outsource.

HOW TAYLORED IS HELPING GOVERNMENTS LIKE YOURS

From a full package of IT managed services to physical security and surveillance, Taylored's expertise and experience makes us uniquely suited to serve the IT needs of Indiana government organizations — from start to finish.

REAL GOVERNMENT EXPERIENCE

When you're dealing with IT systems, one size does not fit all. That's why the needs of a government organization differ greatly from those of a health care clinic, school or retail business. Many MSPs claim to have experience serving government organizations, but they don't show the proof. Here at Taylored, however, we've had years of experience with government clients of all sizes — and we're still actively helping them!



Greenwood Aquatics Center Project: Our experts were able to arm park managers with a full-scale surveillance system capable of navigating design challenges inherent to the site. Through a sophisticated Fluidmesh Network design, we were able to build a comprehensive security solution, complete with a powerful NVR server and Milestone software — as well as 27 indoor/outdoor surveillance cameras.

City of Noblesville: Taylored experts are able to design flexible solutions that meet both our clients' technology needs as well as their budget. For Noblesville, Indiana, we helped customize a reliable and redundant VoIP phone solution. We also upgraded their network infrastructure to help secure and provide enhanced reliability for the growing demand of additional IP devices for the city's present and future needs. And in Noblesville's Federal Hill Commons Park, our experts implemented a video surveillance solution that provides better coverage and recognition using 4K camera technology.

City of Fishers: The City of Fishers, a longtime Taylored Systems customer, chose Taylored Systems to provide the structured cabling, access control and surveillance solutions for their new police department building and many other government sites. For structured cabling, they chose a Berk-Tek/Leviton solution with a lifetime warranty. Taylored Systems worked closely with the City of Fishers IT department to design a new access control system using the cloud-based ISONAS Pure Access system. Through these systems, we helped the police department and other city departments secure 146 doors of access control.

Taylored also provided full IP video surveillance for the new police department and the city at large, which consisted of 67 IP cameras and the Milestone Professional video management platform. Due to the versatility of the platform and our installation expertise, the City of Fishers was able to leverage all their existing IP cameras and bring them over to the Milestone video management solution.

Our partnership with the City of Fishers continues to this day, as we are currently working with city officials to provide these services to the new fire department headquarters, along with several fire stations.

READ MORE CASE STUDIES IN OUR LITTLE BLACK BRAG BOOK >

CUSTOM SOLUTIONS

We don’t believe that one IT solution fits all industries, but we do believe that flexibility is key for strengthening and streamlining your agency operations. Here at Taylored, we never urge our clients to use prepackaged solutions. Especially when it comes to a government organization, a willingness to think outside of the box is key for investing in your security and success. When you partner with us, we’ll integrate your existing IT systems and design custom solutions that fit your needs, budget and processes.

NO UNFORTUNATE SURPRISES

We offer strategic, reliable services so that you can rest assured that there will be no unexpected challenges — budgetary or otherwise.

Budgeting. Government organizations require board approval for IT spending. That’s why our predictable charges and service fees make it easier to develop budgets that best accommodate your needs — with no unhappy surprises.

No downtime. Our 24/7 availability for various critical issues eliminates downtime and ensures that you have help when you need it most.

A LONG HISTORY OF SUCCESS

Here at Taylored, we’ve been helping Indiana businesses and organizations with IT services for over 30 years. We see what we do as less of a business transaction and more of a relationship — after all, your success is our success. We’ve served government organizations for years, so we understand the systematic governmental process and can design customized, high-security solutions for your mission-critical projects. At Taylored, we offer innovative security and data solutions to keep your entire IT infrastructure more safe and efficient — so that you can focus on serving your citizens.

THANKS FOR READING!

We hope you found this information useful and will be able to implement changes in your organization. If you would like a consultation to assist you, please feel free to reach out!

ABOUT US

Taylored Systems is a leader in technology. Our dedicated employees provide clients with innovative voice, data and security solutions. Our solutions are designed with managed services and supported by superior customer service. We measure success by the continued satisfaction of our clients — “our partners” in communication.

TAYLORED SYSTEMS, INC.
14701 CUMBERLAND RD, SUITE 100
NOBLESVILLE, IN 46060

INFO@TAYLORED.COM PHONE: 317-793-2247 FAX: 317-776-4004