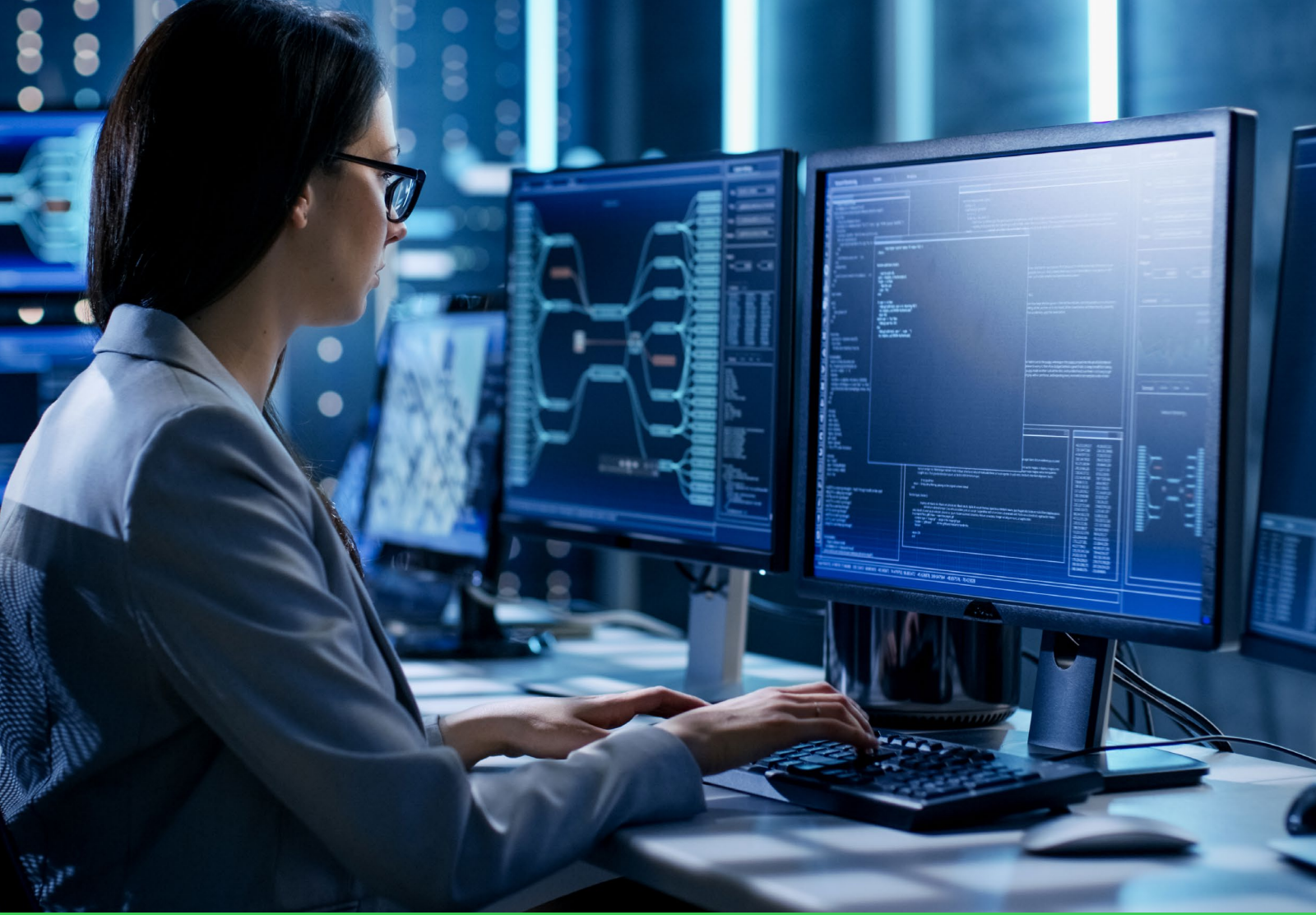


Turning Local Government Cybersecurity Challenges into Opportunities

apc.com/edge

Life Is On | Schneider Electric

Introduction

Today's citizens expect the convenience of personalized digital experiences — using an app to pay for parking or renewing license plates online, for example. Artificial intelligence and machine learning are ideal ways to add new capabilities, but government agencies often face heightened constraints that can make it challenging to adopt and deploy advanced technology quickly. This likely contributes to why **80% of government organizations** are still at the initial or developing digital maturity stages.

Plus, with new and expanded digital platforms come difficulties in identifying funding for upgrades, internal skills gaps, legacy culture and systems to overcome, and new cybersecurity risks. Local government IT executives **recently indicated** that three of their most significant barriers to addressing cybersecurity are:

1. The increasing sophistication of threats
2. Inadequate cybersecurity staffing
3. Decentralized IT and security infrastructure

In this eBook, we'll explore these three challenges and discover how state and local government IT can benefit from a partner who understands how to navigate their unique requirements to break down these barriers and turn cybersecurity challenges into opportunities.

Local Government Cybersecurity Challenge #1: Increasingly Sophisticated Threats

Cybersecurity threats have become increasingly sophisticated, presenting significant challenges for state and local governments. These entities often face budgetary and resource constraints, making it challenging to keep up with rapidly evolving cyber threats. Cybercriminals are now designing multi-faceted, advanced strategies that may combine technical exploits with social engineering. Tactics like ransomware, phishing attacks, and state-sponsored cyber warfare have become more targeted and complex.

Governments handling sensitive data and critical infrastructure are attractive targets for cybercriminals. The necessity for robust cybersecurity measures and continual updates to security protocols has become more crucial than ever to protect against these advanced threats. However, local government IT departments face a significant challenge in keeping their employees up-to-date with the latest cybersecurity training. IT personnel might be tasked with a broad range of responsibilities, leaving less time for specialized training. Plus, cybersecurity can be a complex field, and not all government employees have a technical background. Making the training understandable and engaging for non-technical staff is a significant challenge.

As technology advances, so do the tools and methods used in cybersecurity. Local government IT departments need to adopt a proactive approach to cybersecurity training, which includes regular updates to training programs, allocation of adequate resources, and fostering a culture of continuous learning and vigilance against cyber threats.

Fortunately, **edge computing** offers cybersecurity benefits as innovative and advanced as these new attacks. With real-time device monitoring and automation, less distance for data to travel, and fewer opportunities for threats to compromise it, edge computing is designed with modern cybersecurity at the forefront. Data is processed locally, and lag time is minimized, so unusual activity can be spotted and neutralized more quickly. You may also be able to program devices to take automatic action to protect the network. Edge computing also reduces the number of touchpoints the data passes through and the number of copies made, minimizing the opportunities for interference or interception.

Schneider Electric's **EcoStruxure IT** solution combines real-time monitoring, mobility, and insights to protect your IT infrastructure. You can centralize the management of all networked devices (regardless of vendor), monitor device performance and sensor data, consolidate your alarms to focus on what's important, and get insight into your entire distributed environment's current and future state, helping you get ahead of threats before they happen.

Local Government Cybersecurity Challenge #2: Inadequate Cybersecurity Staffing

Another critical way to stay ahead of the increasing sophistication of state and local government cybersecurity threats is to gain access to advanced skills and expertise. This can be a significant challenge for teams with a limited budget for staffing. Government budgets aren't necessarily focused on funding the technology enabling its programs, especially when it comes to newer, less widely understood technologies like AI and machine learning.

The Public Technology Institute's (PTI) 2023 Local Government Cybersecurity National Survey found that most respondents (52%) do not have an individual whose sole job responsibility is managing cybersecurity efforts. The record-high cybersecurity workforce shortage is likely a key contributor to the skills gaps local governments are facing. The **2023 Cybersecurity Workforce Study** found that the gap between workers needed and workers available increased 12.6% year-over-year.

Recruiting and retaining skilled cybersecurity professionals in the public sector presents unique challenges, which are crucial to understand for effective workforce development. These challenges include:

- **Competition with the Private Sector:** Public sector organizations typically operate under strict budget constraints, limiting their ability to offer competitive salaries and benefits.

- **Rapidly Evolving Threat Landscape:** The cybersecurity field is rapidly evolving, requiring professionals with up-to-date knowledge of the latest threats and technologies. Budget constraintscan also affect the availability of essential training resources.

- **Unique Regulatory Constraints:** Public sector cybersecurity roles often require understanding specific regulatory and compliance issues unique to government operations. Certain government positions may also require security clearances, which can limit the pool of eligible candidates.

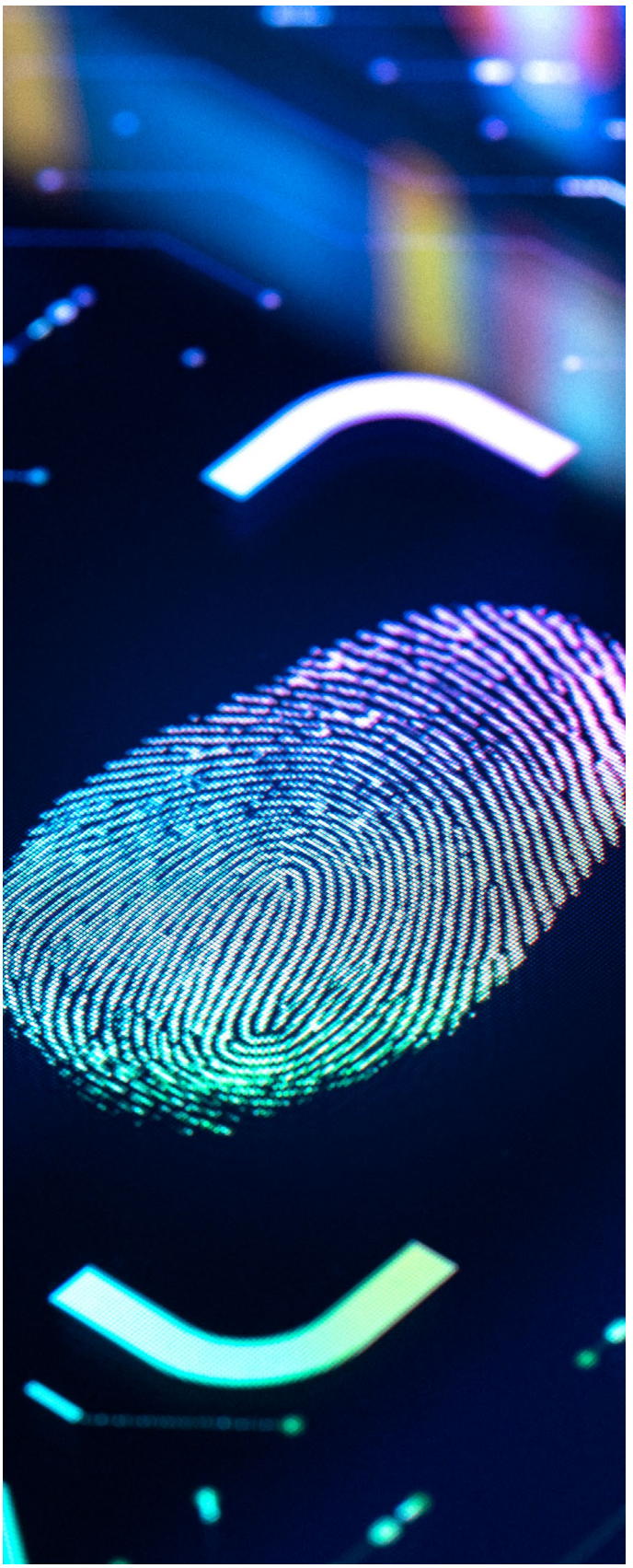
To address skills gaps, 40% of survey respondents said they are engaging vendors to support cybersecurity. Private vendors are becoming a pivotal resource for IT departments to expand their capabilities without breaking their budgets. Even with multiple locations having limited or no IT staff on-site, they can gain greater visibility and control of their entire infrastructure to boost security and uptime.

With the necessity of doing more with fewer resources becoming more common in local government cybersecurity, partnerships with experts and managed service providers like Schneider Electric can make it easier to design the ideal IT kit for this environment and ensure it's all secure. Schneider Electric's unique expertise in **uninterruptible power supplies** (UPS), **data center cooling**, and **physical threat** management is unmatched in terms of making it easier for IT to remotely monitor and manage edge data centers with minimal staffing.

We also have key strategic partnerships with all the major vendors like Stratis, HP, Lenovo, Cisco, and more. Our partners understand the growing importance of local government cybersecurity, so we are uniquely positioned to create all-inclusive solutions. These partnerships make it possible to expand your knowledge base of expertise without investing in full-time talent.

Local Government Cybersecurity Challenge #3: Decentralized IT and Security Infrastructure

Decentralized IT and security infrastructure present a significant challenge for local government cybersecurity and IT personnel. This challenge encompasses several key aspects:

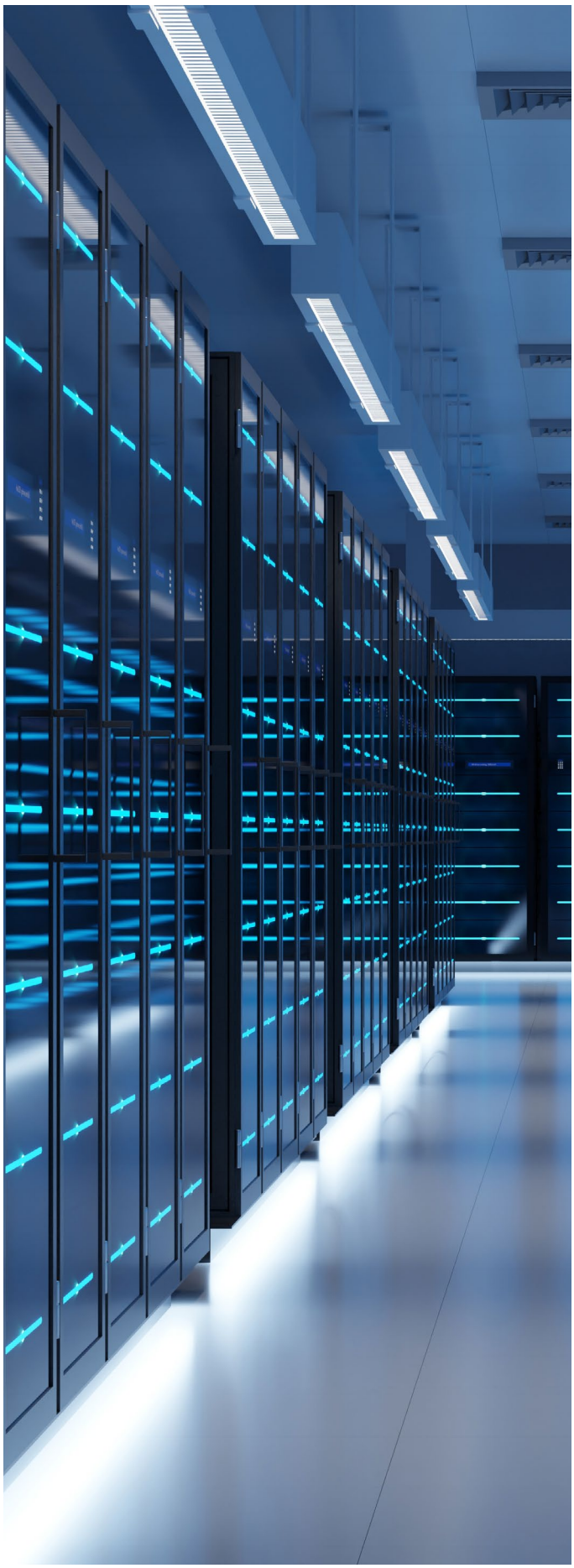


Lack of Standardization

Different departments or agencies within the local government might use diverse technologies and systems in a decentralized environment. This lack of standardization can lead to inconsistencies in security protocols and vulnerabilities that are hard to monitor and manage uniformly because there is no centralized view of all activities and potential vulnerabilities. Each department may have its own tools, software, and processes, making implementing a cohesive cybersecurity strategy across the entire local government challenging. Coordinating responses to cybersecurity incidents can be complicated when systems and data are spread across multiple, independently managed infrastructures.

Resource Allocation and Expertise

In a decentralized setting, resources like funding, personnel, and technical tools may be unevenly distributed. Some departments may lack the resources or expertise to protect their systems adequately. There's also the challenge of ensuring all departments have access to skilled cybersecurity professionals and up-to-date technology.



Compliance and Regulatory Challenges

Ensuring compliance with state and federal cybersecurity regulations becomes more complex in a decentralized environment. Different departments may have varying levels of compliance, leading to potential legal and security risks. It can be difficult to enforce consistent policies and procedures across all departments, essential for meeting regulatory requirements.

Strategies for Addressing These Challenges

Addressing the challenges of decentralized IT and security infrastructure requires a balanced approach that respects the autonomy of individual departments while establishing cohesive, government-wide cybersecurity policies and practices. Developing a unified cybersecurity strategy that can be implemented across different departments while allowing for some level of autonomy is essential. Local government cybersecurity professionals should also prioritize Investing in centralized cybersecurity tools and platforms that can provide visibility and control over the entire network.

Benefits of Decentralization

While decentralization can present challenges, there are also significant benefits to consider. The decentralized edge computing model allows state and local governments to analyze data more efficiently with less latency, which is helpful in situations where quick decisions or actions must be taken (like emergency services.) There are also the cost and cybersecurity benefits that accompany keeping data local. With the right partner, the challenges of decentralized IT can become opportunities.

Four Steps to Controlling Your Remote IT Installations

Local government IT and cybersecurity departments frequently encounter challenges monitoring their dispersed IT infrastructures, resulting in a disorganized and unmonitored landscape where decentralized IT can appear daunting. Contrary to traditional **data centers**, which typically have skilled personnel available around the clock, these remote sites are often overseen by local staff whose expertise may not primarily lie in IT management. In regular operations, these locations tend to operate without sufficient oversight, leading to a lack of comprehensive understanding regarding the installed systems, available capacities, and potential malfunctions.

This is precisely the scenario where Schneider Electric's expertise becomes invaluable. Our solutions provide clarity, control, and expert management to these remote environments, ensuring secure, efficient, and reliable IT operations across all local government installations. Here's our 4-step process for gaining control over your decentralized IT installations:

1. Evaluate Your Current Assets

Our initial approach involves thoroughly examining your existing asset list, typically using the data you provide. Alternatively, we can perform an on-site asset collection or assessment. The former offers a basic site inventory detailing asset age, status, part number, and serial number. The latter, however, entails a more in-depth analysis of your IT environment, encompassing evaluations of power and cooling efficiency, comprehensive inventories, spatial layouts, photographic documentation, and tailored recommendations.

2. Determine Your Needs

After completing the inventory and site evaluations, we propose strategies to elevate your sites to meet industry standards. Schneider Electric is equipped to seamlessly manage any enhancements to your IT Infrastructure systems, offering a complete, turn-key solution.

3. Connect Sites to Our Experts

A viable strategy to safeguard the integrity of your remote IT infrastructure is to integrate all pertinent devices with Schneider Electric's StruxureOn service. This connection links your infrastructure systems to our specialists for proactive 24/7 monitoring of any system irregularities and ensures accessibility through the StruxureOn mobile app. This direct link to Schneider Electric's customer service facilitates swift resolution of issues.

4. Manage Infrastructure Systems

This scenario might sound familiar: You oversee a vast array of IT Infrastructure systems, face limited on-site staffing, and encounter continuous operational challenges. Remote incident management is vital to maintaining focus for your local staff on their primary duties, ensuring system functionality, and sustaining business operations. Schneider Electric steps in here with our Infrastructure Fleet Management. An extension of the StruxureOn service, Fleet Management includes on-site resolution of system issues. This proactive service plan not only anticipates and mitigates potential business-impacting events, but also significantly reduces Help Desk inquiries and the average time required for repairs.

Get Personalized Guidance for State & Local Government Cybersecurity

Schneider Electric is recognized as a global leader in IT infrastructure and digital solutions, and with strategic partnerships with all the major vendors, we are uniquely positioned to create all-inclusive solutions that meet the unique requirements needed by local government cybersecurity and IT teams.

If you're ready to start the conversation about taking small steps today to enable big changes tomorrow, **contact Schneider Electric here** or call us at 1 (877) 800-4272.

Schneider Electric provides **TAA-Compliant Offers** that meet the requirements of the Trade Agreements Act (TAA). The TAA is intended to foster fair and open international trade. It requires that all products be produced or undergo "substantial transformation" within the United States or a designated country.

Life Is On | Schneider Electric

We can help you tackle anything, from basic preventive services all the way to redesigning your permanent IT backbone.

Call us at 1 (877) 800-4272 to get started, or check out our partner selector tool to find a partner ready to support you.

apc.com/edge

Schneider Electric

Boston One Campus
800 Federal Street
Andover, MA. 01810 USA
Phone: + 1 976 794 0600

www.apc.com

998-23146502_LMA-US