COMCAST
BUSINESS
Powering Possibilities™

Cybersecurity best practices for state and local agencies

As state and local governments grapple with increasingly sophisticated cyber threats and limited resources, they are harnessing managed security services to enhance their cybersecurity defenses.

Cybersecurity is top of mind for SLGs as cyberattacks continue to grow more sophisticated and frequent. Moreover, recent high-profile attacks targeting both commercial and government organizations have heightened awareness and underscored the urgent need to better understand and secure mission-critical operations.

As agency leaders look to address this increasingly complex landscape, however, they face unique challenges. With limited resources, many municipalities find it challenging to implement modern cybersecurity solutions. Yet, the need to protect sensitive data and ensure the continuity of essential services has never been more critical.

In fact, a survey of more than 4,000 state, local, tribal and territorial government organizations on cybersecurity preparedness from the Center of Internet Security showed that 70% of respondents feel they lack the sufficient funding and resources to combat evolving ransomware attacks.
Amid numerous competing priorities and the need to align everyone from executives to security practitioners, SLGs are turning to a range of solutions to bolster their cybersecurity defenses, including Secure SD-WAN, Unified Threat Management (UTM) and Managed Detection and Response (MDR).

Growing threats to SLGs

From ransomware attacks that paralyze city services to the growing vulnerabilities posed by connected devices, SLGs are under siege from increasingly complex cyber threats. With over 90,000 local government entities across the United States, the sheer scale of operations makes them vulnerable as cybercriminals continuously refine their methods of attack.

According to the 2024 Comcast Business Cybersecurity Threat Report, phishing and credential theft are now the primary tactics used to gain access to networks, leading to increased breaches and spurring the need for rapid detection of bad actors once inside the network.

“Attacks against the network perimeter are still a big concern, but the fact is that it’s much easier to land inside using phishing because humans can be the weakest link,” said Ivan Shefrin, Executive Director of Managed Security Services for Comcast Business. “It’s usually not a question of if but when adversaries will penetrate a network.”

Additionally, the rise of unmanaged Internet of Things (IoT) devices — such as surveillance and body cameras — has introduced additional network vulnerabilities. These devices, if compromised, can provide cybercriminals with lateral access to more sensitive parts of the network.

“[These] problems are compounded by legacy IT infrastructure that is so prevalent across many SLG entities, but highly vulnerable to cybersecurity attacks,” Shefrin added.

Outdated infrastructure makes it difficult to implement modern security measures, which increases the risk of unauthorized access to sensitive data and critical systems. For most smaller municipalities, limited funding and staffing can prevent 24/7 network monitoring, leaving them exposed to cyberattacks and prime targets for cybercriminals. As a result, addressing cybersecurity for these governments is more critical than ever.

A defense-in-depth approach to cybersecurity

Given the relentless nature of modern cyber threats, SLGs require a multi-layered, proactive defense strategy to stay ahead of potential breaches. Known as "defense-in-depth," this approach involves implementing multiple security controls to create a comprehensive shield around critical applications, data and services.

"Defense-in-depth is based on the idea that no single security product can fully protect against all potential attacks, so multiple layers are needed to stop threats," said Shefrin. This principle is particularly vital for SLGs, which are often resource-constrained and more vulnerable to increasingly sophisticated cybercriminals.

To begin, SLGs should conduct a comprehensive security assessment to pinpoint weaknesses and risks. Based on these insights, they can implement key solutions like Multi-Factor Authentication (MFA) and zero-trust access controls to ensure that only authorized users can interact with sensitive data, significantly lowering the risk of breaches.

Additionally, tools like Endpoint Detection and Response (EDR), DDoS Mitigation and MDR provide crucial real-time monitoring and threat detection, allowing agencies to act quickly to prevent incidents from escalating.

"With our adversaries now using Generative AI and Domain Generation Algorithms (DGAs) to create ever more sophisticated phishing and spear phishing campaigns, it's now more critical than ever for SLGs to monitor their IT environments 24/7 using solutions such as EDR, XDR and MDR," Shefrin said. "Advanced detection and response services can help SLGs contain and disrupt attacks once attackers land inside the network perimeter but before a significant data breach occurs."

"It's usually not a question of if but when adversaries will penetrate a protected network."

> Ivan Shefrin, Executive Director, Managed Security Services, Comcast Business

Shefrin also highlighted the importance of leveraging external resources like the Multi-State Information Sharing and Analysis Center (MS-ISAC), which offers threat intelligence, security monitoring and response capabilities tailored specifically for SLGs.

By adopting a defense-in-depth strategy, SLGs can strengthen their cybersecurity posture and better protect their digital infrastructure in the face of increasingly complex cyber attacks.

Comcast Business's comprehensive solutions

For state and local agencies seeking to transform their defenses, Comcast offers a modernized approach to cybersecurity, combining advanced technology with hands-on support to help protect networks from today's dangerous threats.

At the core of this effort is Comcast Business's MDR service. The 24/7 monitoring system goes beyond just keeping an eye on networks — it helps safeguard IT ecosystems, covering everything from cloud services, applications and databases to remote access and user identities.

When paired with additional tools like EDR, zero-trust access controls and next-generation UTM firewalls, SLGs benefit from a layered defense that proactively detects, contains and mitigates threats before they escalate. As Shefrin noted, this is "the most comprehensive and recommended approach that includes not only endpoint and network, but also cloud, identity, applications, databases, remote access and other critical infrastructure."

What distinguishes Comcast Business is its ability to scale these solutions to meet the demands of large government entities. Last year alone, for example, Comcast Business leveraged its expansive network and advanced threat intelligence to prevent 29 billion cyberattacks for its security customers across segments.

In one instance, after being hit with a cyber attack, one SLG spoke with Comcast Business about closing gaps in their network and cybersecurity posture across nearly 50 locations.

Comcast provided a solution encompassing Secure SD-WAN, next generation UTM firewalls, connectivity, and DDoS Mitigation Services. The solution enhanced the SLG's security posture, and improved network performance.

By combining cutting-edge technology with dedicated support, Comcast Business can help alleviate the pressure on government IT teams, enabling them to shift focus from reactive troubleshooting to proactive strategy. For SLGs aiming to secure their digital environments, Comcast Business provides the solutions and expertise they need in an ever-evolving cyber landscape.

> **Learn more** about how Comcast Business is helping state and local governments secure their data and experiences.