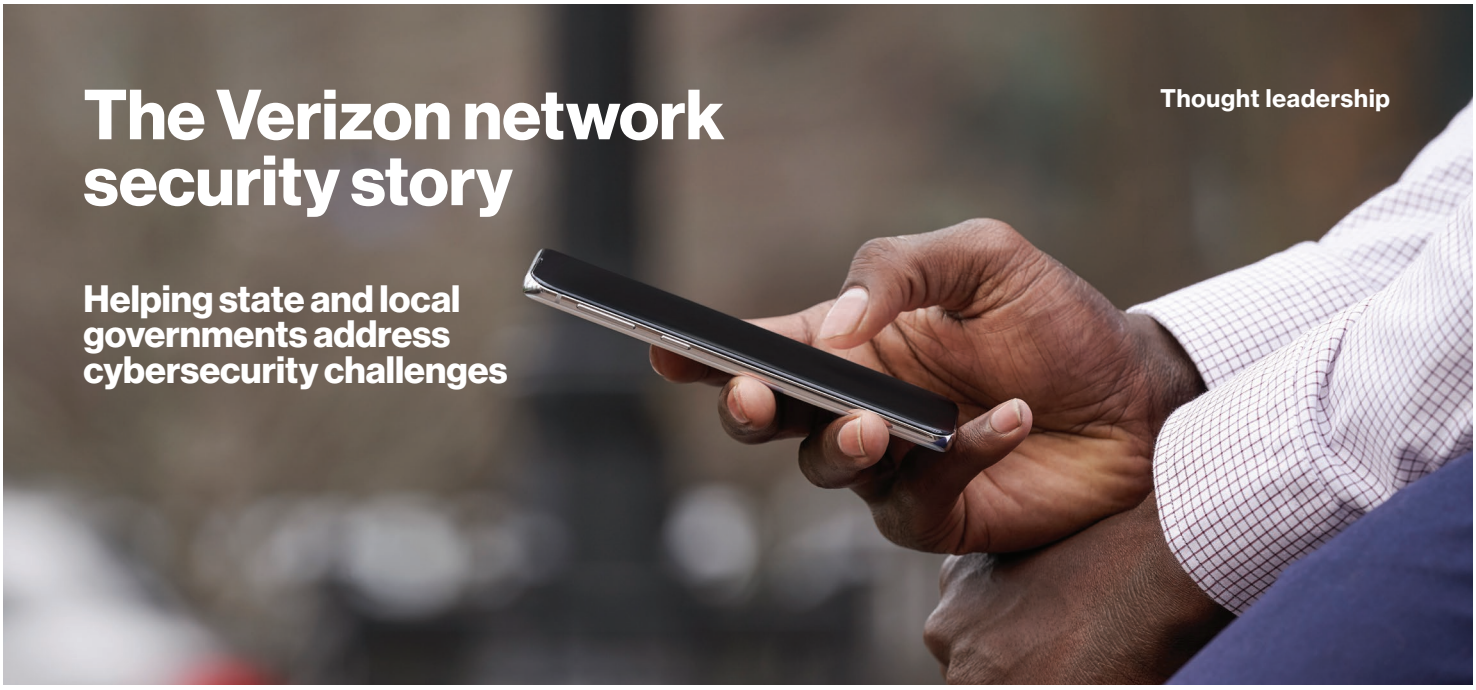

The Verizon network security story

Thought leadership

Helping state and local governments address cybersecurity challenges

Cybersecurity is a vital issue for commercial entities of all sizes, from small businesses to major enterprises. But cybersecurity takes on even more importance in the public sector, where critical citizen services—including voting and 911 dispatch systems—can be at risk. Additionally, states, cities, and towns have to protect citizen information and public funds from theft, or they stand to lose the public's trust. To stay protected, state and local agencies need to make security a priority, now more than ever.

The challenge: cybercrime remains on the rise

The 2020 Verizon Data Breach Investigations Report lists 6,843 major cybersecurity incidents in the public sector, including a large percentage of ransomware attacks—61% of all malware cases. These statistics tell only part of the story. When state and local governments are the victim of cyberattacks, it can be devastating, disruptive—and expensive. Consider the following:

A high-profile ransomware attack on Baltimore, Maryland
The Baltimore ransomware attack occured in May, 2019, costing an estimated $18.2 million—a combination of lost or delayed revenue and direct costs to restore systems. The attack stopped city business and citizen services for weeks.[1]

New Bedford, Massachusetts ransomware attack
New Bedford was hit by a ransomware attack in July, 2019, with hackers demanding $5.3 million in bitcoin to release the city's data. Thanks to delaying tactics, the city managed to negotiate with the attackers and paid $400,000 to get its files back.[2] Beyond the ransom money, the incident disrupted city services.

22 Texas towns attacked
In August, 2019, 22 Texas towns were simultaneously hit with ransomware attacks and held hostage for millions of dollars after hackers infiltrated their computer systems with malware and encrypted their data. The attack triggered a statewide disaster response from the National Guard and the F.B.I.[3]

Allentown, Pennsylvania hacked
In 2018, Ukrainian hackers attacked Allentown, Pennsylvania with malware that shut down the city's computer network for weeks. How did it happen? An employee took a laptop with him while traveling, unwittingly clicked on a phishing email, and the malware spread rapidly when he returned to the office. While no ransom was demanded, the attack cost $1 million to clean up, and improved defense now costs $420,000 a year, putting the city's budget under pressure.[4]

There are many more stories of cyberattacks on small towns and major cities. Though the details vary, there are recurring themes—critical citizen services disrupted (including public safety), municipalities scrambling to respond, significant financial impact, and reputational loss.

> **"Most of these attacks are due to vulnerabilities, gaps in operational security, and overall weak infrastructure discovered and exploited by cybercriminals."**
>
> – from a recent report from Malwarebytes Labs.[5]

As for the attacks, they share a common theme as well. According to a recent report from Malwarebytes Labs,[5] "They often gain a foothold into the organization through ensnaring employees in phishing campaigns and infecting endpoints, or having enough confidence to launch a spear phishing campaign against high-profile targets in the organization."

verizon

Why are cybercriminals targeting state and local governments?

There are several important reasons:

Municipalities seem easier to hack.
Hackers consider state and local agencies a softer target than commercial enterprises, since they may lack advanced security technology or expertise. Often short of funds, they may not be able to allocate the capital necessary to prevent attacks. According to a study conducted by the National Association of State Information Officers (NASCIO), 50% of states do not have a committed cybersecurity line-item in their budgets—paralleling a lack of funding at the municipal level. And during a talent shortage, it's hard for state and local agencies to attract and retain experienced security personnel.

Municipalities have valuable data.
Local governments record large amounts of data—voter records, financial and personal information—which is attractive and potentially valuable to hackers. Hackers have a strong track record of success gaining access and extorting funds from municipalities (see previous stories). In fact, two-thirds of ransomware attacks targeted state and local governments in 2019, according to Barracuda Networks, an IT security firm,[6] with the average payout on the rise.

Citizen self-service opens new vulnerabilities.
More and more services are now offered online at all levels, bringing new convenience to citizens, but creating possible gateways for fraudsters and hackers.

COVID-19 means more scams.
Any crisis—but particularly a global pandemic—is an opportunity for scammers, according to Stephanie Helm, the director of the MassCyberCenter in Massachusetts. "Hackers have been tailoring their attack vectors and their phishing emails to use the COVID-19 tragedy to get people to click on links that they shouldn't open," Helm said. Also, in response to the coronavirus pandemic, more and more government workers at all levels are working remotely, creating new vulnerabilities as they rely on unsecured laptops and public networks.

The bottom line?

Cybercriminals take advantage of human nature and network vulnerabilities. Human nature can be hard to change. Public sector employees have to become more vigilant to spot any potential scam—a request for sign-in credentials that claims to be from a cohort, an email asking for the recipient to click (and install malware), or other more sophisticated scams. This level of skepticism—and technical savvy—may not be part of every employee's DNA, though training can help. And when addressing network vulnerabilities, Verizon can make a big difference.

The solution: Verizon network security expertise and solutions

Stopping cyberthreats seems simple—protect the network so that only authorized users can gain access. But in the context of public sector, the challenge is much more complicated. There's a global cyber talent shortage, and states and municipalities are often outbid by deep-pocketed private sector businesses. As a result, smaller public sector agencies may find it difficult to hire and retain the resources (human and technological) necessary to secure their network and protect their data from cybertheft. Plus, state and local agencies are inherently more vulnerable now that more agency employees are working remotely—often without enough protection. All it takes is one laptop infected with malware and suddenly the whole organization can be paralyzed.

A trusted partner for end-to-end security before, during, and beyond COVID-19

Verizon serves as a trusted partner to its public sector customers, providing reliable connectivity, end-to-end security, unparalleled expertise, and a wide range of services. Now Verizon is helping government agencies at all levels address cybersecurity during a challenging time when it's even more critical to keep communication, collaboration, and citizen services secure.

Why Verizon? The Verizon security story

While much of the world knows Verizon primarily for its innovative wireless solutions, Verizon is also recognized as a leading global provider of cybersecurity services. Verizon taps its vast global network and more than 25 years of security experience to analyze attack trends and activity, helping organizations make more informed, data-driven decisions about security. Verizon delivers comprehensive threat intel and response capabilities to a wide range of organizations—including state and local agencies throughout the US and Fortune 1000 companies around the globe. That's how Verizon has become such a trusted voice in security—one that consistently garners recognition in the industry.

Security insights gleaned from a global network

Being a telecom leader means keeping the network secure, since Verizon customers rely on fast connectivity, availability, and reliability. Through a relentless focus on the security of its own network, Verizon has gained significant insights and expertise on all aspects of security and cyberthreats—and how to address them. The sheer magnitude of Verizon's network means more security expertise, and ultimately, security offerings. For example, Verizon's 4G LTE network now covers more than 2.6 million square miles and 98% of the U.S. population.[7]

Verizon gains broad and deep security insights from protecting its network. After all, security is an ongoing battle, and Verizon is on the frontlines, every day—protecting its network, and gathering invaluable insights and exceptional expertise that can help Verizon's public sector customers stay secure and protected.

verizon

Turning cybersecurity expertise into actionable insights

One high-profile example of Verizon's cybersecurity expertise is the annual Data Breach Investigations Report (DBIR), which provides a crucial, in-depth look at the latest cybercrime techniques and tactics and its companion Public Sector and Education Snapshots. Over the last decade, the Verizon DBIR has become an industry-standard security resource. It offers a comprehensive look at methods cybercriminals commonly use to infiltrate both private and public computer networks—as well as the best ways to thwart their behavior.

Verizon provides this invaluable resource at no cost. Municipalities can use the results of this year's DBIR as a platform to improve awareness of the latest tactics used by cybercriminals, to understand what threats are most relevant, and to evangelize and garner support for security initiatives.

To review the latest report, go to:
enterprise.verizon.com/resources/reports/dbir/

Making a significant investment in security

Recognizing the importance of specialized security expertise, Verizon has made significant ongoing investments and acquisitions to remain the leader in managed security services. This continual investment—from accelerating detection to automating security processes to creating AI-driven security tools—means that Verizon can offer comprehensive security that goes far beyond point-solution providers.

Verizon solution portfolio: delivering end-to-end security

What can Verizon and its security expertise bring to your state or local agency? Verizon can deliver comprehensive security that covers the full continuum of security needs—with advanced offerings in each key area, creating end-to-end security. Verizon structures its security offerings based on the four-pillar model developed by the National Institute of Standards and Technology (NIST) and adopted widely as a core cybersecurity framework.

Identify
Enhance your visibility of cyber risk

Protect
Protect the attack surface

Detect & Respond
Detect and respond to cyber attacks faster

Recover
Minimize impact and quickly restore operations

Consider what these four areas mean to your agency:

Identify
Knowledge is power, of course. Knowing about security vulnerabilities empowers you to stop hackers and others intent on creating mayhem—and stealing funds. Protect your agency by understanding your vulnerabilities. If you know the issues, then they can be addressed.

Protect
End-to-end security helps ensure constant protection, giving you the peace of mind that lets you focus on the more pressing day-to-day business of governance. Staying protected from attacks is especially critical during vulnerable periods, such as health emergencies, elections, and periods of economic instability, which often inspire higher levels of cyberattacks.

Detect & Respond
Slow detection and response gives hackers the time they need to capture more control over your network and data. Fast, thorough detection minimizes impact, while fast response shows that your agency is aware and responsive to all threats.

Recover
Slow recovery time is expensive and keeps internal processes and citizen services at a standstill. Fast recovery shows resilience and short-circuits a period of public embarrassment, when key citizen services are not available.

A full portfolio of security solutions

Every state or local agency is at a different point in terms of security. Some have focused extensively on security, since it's critical to their success. For example, a state Board of Elections knows that the security of its infrastructure is vital to a fair election. Other municipalities may not have the time or resources to explore security. Verizon's broad portfolio of security solutions enables it to deliver precisely what each public sector client needs—no matter where they are along the path from vulnerable to protected.

Verizon's security solutions architects are highly trained and skilled in designing solutions that take full advantage of all networked-based security capabilities—and that meet the needs of today's state and local agencies. Here are just a few of the offerings within the Verizon security portfolio:

Identify

Cybersecurity Assessment
Verizon helps public sector organizations focus on defending against the most likely and probable threats. This assessment helps provide the valuable data that enables state and local agencies to determine where to focus their attention—and what security initiatives to pursue.

Cyber Risk Monitoring
Cyber Risk Monitoring assesses your security using quantified scoring algorithms, detailed dark web findings, and proprietary data from Verizon's threat intelligence library. It gives you the data you need to identify security gaps and evaluate where you need to focus, all leading to more informed decisions.

verizon

Protect

Network security monitoring and network security management services
Verizon's network security monitoring and network security management services are designed to help you keep ahead of threats while reducing the workload. Verizon helps keep your applications up to date, properly configured and secure. Deep visibility into the global threat environment gives Verizon the experience and awareness to spot many potential threats before they happen, all while keeping security costs under control.

Detect & Respond

Rapid Response Retainer
This core service package consists of essential components, such as a proactive assessment, emergency escalation protocol, and guaranteed service level agreement. Its modular nature allows agencies to design a retainer that matches their needs. Add-on services—such as incident response planning, or detection and response capabilities on the network (backbone or endpoint)—provide customization options that help minimize the time to contain and recover from a cyberattack.

Recover

Verizon's Security Professional Services (SPS)
The SPS team helps hundreds of organizations achieve and maintain compliance with a wide range of regulations, as well as evaluating and refining their security architecture and processes. The SPS team is also world-renowned for its incident response team and forensics capabilities, should your agency experience a data breach.

As with all governmental purchasing, agencies will need to confirm what services are available via their state contract(s).

Expanding security offerings to meet ongoing, evolving security challenges

To retain and expand its leadership role, Verizon continues to make major investments in security services, including the acquisition and integration of new organizations, such as ProtectWise and Niddel. It continues to create new offerings, such as the Cyber Risk Monitoring service and Managed Detection and Response. It continues to innovate, using new technologies and approaches (e.g., blockchain-based principles) in its products. And Verizon continues to expand its security offerings via strategic partnerships with a wide range of world-class vendors.

Next steps: Verizon is ready to strengthen your security

Verizon understands the needs of the public sector, and already serves as a trusted partner to hundreds of cities and states that rely on the robust, end-to-end security that Verizon offers. To stay secure and protected against all threats, choose a thought leader, an acknowledged security expert, and a trusted advisor. Choose Verizon.

Ensuring security for state and local agencies

Verizon is providing secure solutions that help states and municipalities take on strategic initiatives, including:

- Making voting more secure
- Keeping citizen communications and payments secure
- Securing emergency communications (including 911 communication centers.)
- Ensuring the security of mobile workforces
- Enabling secure remote learning
- Strengthening the resilience of state & local agencies
- Establishing secure virtual contact centers
- Protecting municipalities from global cyberthreats

Learn more

To learn more about how to evolve your security strategy, please contact your Verizon Account Representative.

enterprise.verizon.com/products/security

verizon✓

1 "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts," Baltimore Sun, May 29, 2019. Source: https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html

2 "Town Avoids Paying Massive $5 Million Ransom in Cyberattack," NPR, September 6, 2019. Source: https://www.npr.org/2019/09/06/758399814/town-avoids-paying-massive-5-million-ransom-in-cyberattack

3 "Ransomware Attacks Are Testing Resolve of Cities Across America," New York Times, August 22, 2019. Source: https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

4 "Allentown Struggles with $1 Million Cyber-Attack," Infosecurity Magazine, February 20, 2018. Source: https://www.infosecurity-magazine.com/news/allentown-struggles-with-1-million/

5 "Ransomware Isn't Just a Big City Problem," Malwarebytes, May 30, 2019. Source: https://blog.malwarebytes.com/ransomware/2019/05/ransomware-isnt-just-a-big-city-problem/

6 "Report: Two-thirds of Ransomware Attacks in 2019 Targeted State and Local Governments," Statescoop, August 28, 2019. Source: https://statescoop.com/report-70-percent-of-ransomware-attacks-in-2019-hit-state-and-local-governments/

7 Source: https://www.verizon.com/articles/why-choose-verizon-wireless/