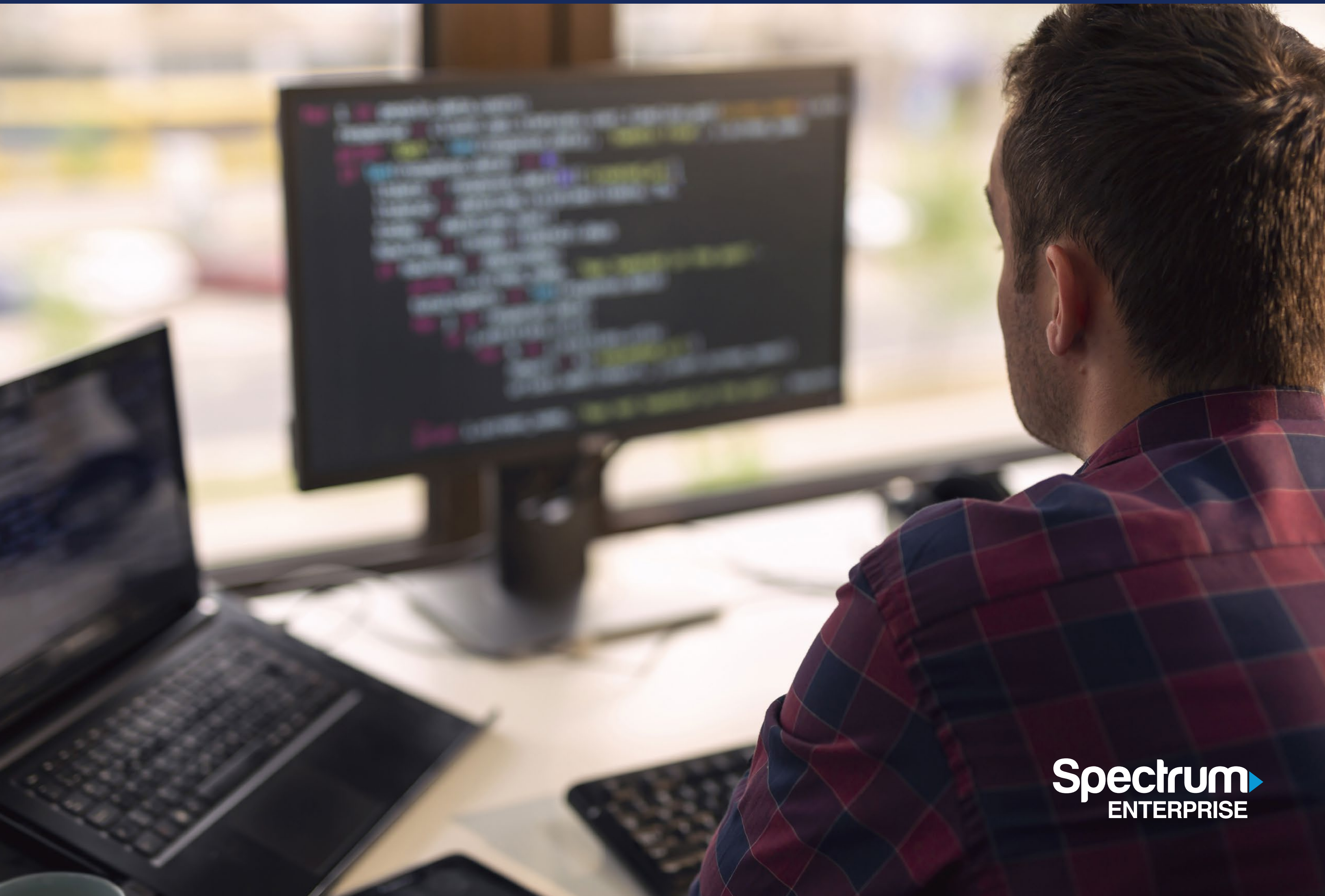
GUIDE

Cybersecurity resources for state and local governments



Spectrum ENTERPRISE

For hackers and malicious actors focused on the state and local government sector, 2020 proved to be a fruitful year — and 2021 is following the same pattern.

Cybersecurity experts reported that 2020 was the largest year on record for DDoS attacks.[1] Minnesota's IT leaders learned this firsthand when their state's networks were inundated with malicious traffic in an attempt to knock government agencies offline that spring.[2] In 2021, cybersecurity analysts reported that DDoS attacks targeting government administration and public sector websites grew by 491 percent in the second quarter compared to the same period the year before.[3]

Sensitive information in government systems is another enticing target for bad actors and 25 percent of cyberattacks on government during 2020 were attempted data theft and leaks.[4] Defending against these ongoing threats to government agencies can seem especially daunting when the tools used by attackers are ever changing. In January 2021, more than 17 million new types of malware and potentially unwanted applications were found by cybersecurity experts.[5]

324 days is the average time for a public sector organization to detect and contain a data breach caused by a malicious attack.[6]

Not only are cyberattacks increasing, but resource-constrained state and local governments must also meet the increasing demand from citizens for 24/7 digital services and access to data. They must also balance compliance requirements from FedRAMP, CJIS and FISMA. However, even for resource-constrained state and local governments, being prepared for cybersecurity threats and staying on top of the emerging cyber threat landscape doesn't have to be daunting or costly. There are many free resources available to help.

Resources to leverage

Multi-State Information Sharing and Analysis Center (MS-ISAC®)

As part of the Center for Internet Security, Inc. (CIS®), MS-ISAC aims to enhance the ability of state and local governments to prevent, protect, respond and recover from cybersecurity attacks. Its website includes cybersecurity best practices, tools and information on threats.

Featured tool: CIS RAM
The Center for Internet Security® Risk Assessment Method (CIS RAM) provides instructions, examples, templates and exercises for conducting a cyber risk assessment. It lets users model foreseeable threats, analyze risks based on attack paths and model threats against information assets.

Cybersecurity & Infrastructure Security Agency (CISA)

CISA is responsible for protecting the nation's critical infrastructure from physical and cyber threats. The CISA has several sub-programs and centers, such as the Cyber Information Sharing and Collaboration Program (CISCP) and the National Information Exhange Model (NIEM). Through these efforts, state and local governments can access trainings, risk and vulnerability assessments, operational planning and incident response, information on state-sponsored threat actors, recovery support and more.

Featured tool: Cyber Resilience Review
This is an interview-based assessment across 10 domains, including asset management, controls management, risk management, training and awareness, situational awareness and vulnerability management. The Cyber Resilience Review provides you with a final report of where your state and local government agency stands with regards to cybersecurity and what you can do to improve it.

National Association of State Chief Information Officers (NASCIO)

Geared toward state governments, NASCIO provides basic guidelines for appropriate access to and the usage of state systems. However, these guidelines can also assist local governments as they look to tighten their cybersecurity controls.

Featured tool: Stronger Together: State and Local Cybersecurity Collaboration Report
While not strictly a tool, the State and Local Cybersecurity Collaboration Report is a free download created in conjunction with the National Governors Association (NGA). This report includes examples of state governments that have created multi-disciplinary approaches to cybersecurity. Most importantly, it also provides 20 actionable security guidelines that can be used by both state and local governments.

Are you prepared?

With the increase in targeted attacks on state and local government IT systems, cybersecurity is no longer just an IT issue. It has become an issue that involves everyone in the organization who accesses them. For state and local governments, cybersecurity is a security and safety risk that must be mitigated at every level.

As the cyber threat landscape continues to evolve and malicious actors come up with new ways to access systems, make sure that you are prepared to foil them and respond should the worst happen. Learn how the government IT solutions experts at Spectrum Enterprise can help at enterprise.spectrum.com/government.

[1] "Distributed Denial of Service (DDoS) Attacks: A Cheat Sheet," Tech Republic, Jan. 29, 2021.

[2] Benjamin Freed, "Minnesota IT Officials Respond to Weekend DDoS Attacks Against State Systems," StateScoop, June 1, 2020.

[3] Vivek Ganti and Omer Yoachimik, "DDoS Attack Trends for 2021 Q2," Cloudflare, July 20, 2021.

[4] Limor Kessem, "Threat Actors' Most Targeted Industries in 2020: Finance, Manufacturing and Energy," March 31, 2021.

[5] "Malware," AV-TEST Institute, accessed Sept. 13, 2021.

[6] "Cost of a Data Breach Report," IBM, 2020.

About Spectrum Enterprise
Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply. Subject to change without notice.

Spectrum ENTERPRISE