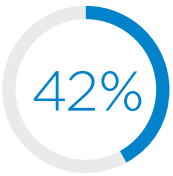
GUIDE

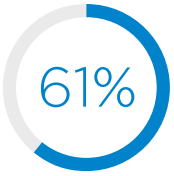
How to stay a step ahead of cybersecurity threats in government

Spectrum ENTERPRISE

of state CISOs are not very confident in the cybersecurity practices at state and local government organizations.[2]



of state IT leaders report inadequate staffing is a top barrier to cybersecurity.[3]



of security and IT leaders are concerned about an increase in cyber attacks targeting employees using home networks and devices.[4]

A wide range of internal and external forces are changing the way state and local governments manage network security.

Pressure is increasing on these organizations to provide easy and convenient digital data access to constituents. At the same time, government networks are increasingly integrating Internet of Things (IoT) devices — sensors, automated controls and other tools — that have the potential to make networks vulnerable.

The high value of the data housed on government networks makes them a favored cybersecurity target, and state and local governments find themselves poorly protected compared to their private sector enterprise counterparts. Some are challenged by maintaining and securing legacy systems, while others are stymied by a lack of resources. Government leaders say that finding staff with cybersecurity expertise is also holding them back.[1]

Even governments with security expertise need to continually adapt. The threats targeting state and local governments are constantly evolving. The profiles of distributed denial of service (DDoS) attacks, ransomware and email spoofing are changing as cybercriminals tap new technology and develop clever workarounds to gain access to and steal sensitive data.

Attacks can have devastating results: Entire applications and services may be rendered useless, and the cost to recover can be in the millions of dollars.

Tracking evolving threats

To protect your organization, it pays to understand today's threats and the trends shaping tomorrow's network data breach attempts including:

Ransomware: The FBI reports that an ever-evolving universe of email scams are difficult to spot. Access through emails, plus brute force entry to networks, lets cybercriminals insert malware into government organizations.

Polymorphic malware: In January 2021, cybersecurity experts found 15,224,388 types of new malware and potentially unwanted applications.[5] It's estimated that 97 percent of all malware now employs some form of polymorphic virus designed to circumvent antivirus software with continuously changing methods to evade detection.[6]

Email spoofing: While email spoofing traditionally impersonated banks, cybercriminals are now masquerading as SaaS companies to steal credentials and access sensitive information.

Advanced persistent threats (APTs): APTs are attacks in which a network is compromised and data is mined over time without knowledge of the organization. APTs have also escalated from compromising a single computer to taking over whole networks in just a few hours.

DDoS: DDoS attacks take many forms and attack all industries. Volumetric DDoS assaults flood networks to bring them down, but other, more-subtle tactics are also in play. For example, DDoS attacks may be conducted via group chats, sending bursts of malicious content rather than a sustained attack.

Budget constraints are the top obstacle for the public sector when it comes to maintaining cybersecurity, followed by complex internal environments and competing priorities.[7]

Real-world cyberattacks

Details of government cybercrimes help paint a clear picture of the evolving threat. Read these examples and see how governments might have been better protected against an attack.

Ransomware closed citizen-facing systems

Type of breach: A ransomware attack took a city government's data and systems hostage. The cybercriminals demanded upward of $50,000 in bitcoin to decrypt the data.

What was lost: Citizen-facing applications — including ones used to pay bills, access court-related information and apply for business licenses and renewals — were taken offline. Affected internal systems included the city's payroll application. These systems and applications were offline for five days. The city spent millions of dollars on emergency efforts to respond to the ransomware attack.

What might have mitigated or thwarted the attack: Multifactor authentication and segmented security zones within the network could have hindered bad actors from moving laterally if they gained access to one device. Use of antivirus software and a next-generation firewall, as well as content scanning and filtering on mail servers, could have protected critical data and prevented intrusion.

Malware infected devices at multiple state agencies

Type of breach: A phishing email distributed malware to infect several hundred devices at three state agencies.

What was lost: Computers crashed and experienced technical issues at the Department of Children, Youth and Families; the Department of Human Services; and the Department of Behavioral Healthcare, Developmental Disabilities and Hospitals. Most of the computers that were impacted were PCs with lower processing power.

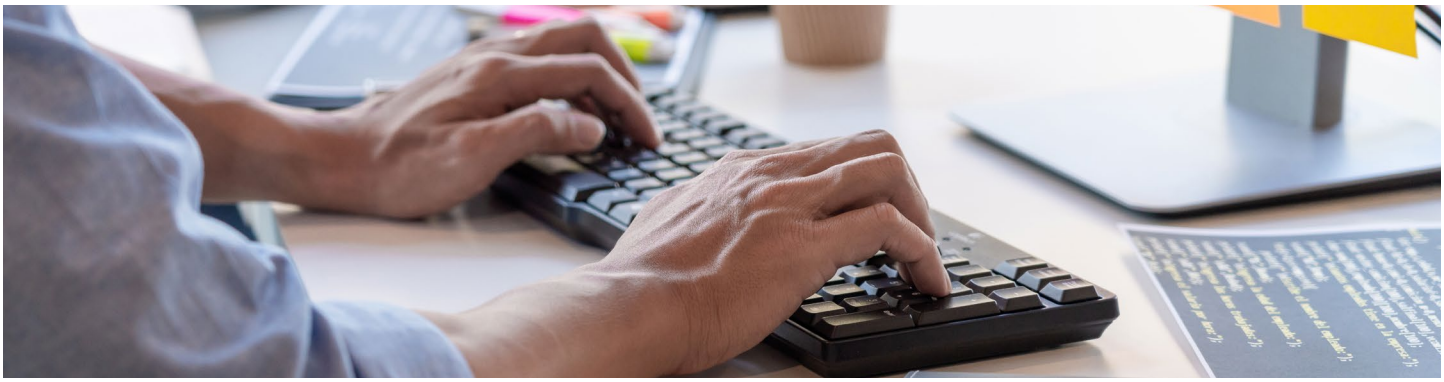
What might have mitigated or thwarted the attack: A next-generation firewall may have prevented the attack.

DDoS shut down city and safety services

Type of breach: A DDoS attack flooded servers for city and police departments.

What was lost: The attack rendered both city websites useless, causing significant downtime and interrupting the city's emergency broadcasting capabilities. City officials spent four days restoring the websites, only to have them attacked again.

What might have mitigated or thwarted the attack: Security help from a managed service provider (MSP) could have blocked the offending IP address and prevented a second attack. With the address blocked, clean traffic would be allowed to pass, which would have enabled city sites to continue operations.



Finding the right protection

Continually keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. That includes unified threat management (UTM), DDoS protection and the support of a network services provider to deliver managed service solutions.

When it's time to evaluate a provider and its services, ask the following questions to help you find the best protection possible:

- What protection do you provide against DDoS attacks?
- After a DDoS attack, do you have a means of letting us continue to work productively on the parts of the network that were not affected?
- How do you identify and mitigate network threats? Can you scan our network for attacks and drain suspicious traffic?
- How can you protect us from malware, phishing and other common cyberattacks on state and local governments?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic between our various sites as well?
- Is a next-generation firewall part of what you offer? What does it provide?
- How will you integrate with our existing network and authentication sources?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- Threats are evolving, and our network is always changing and growing. Can you support us and our investment as the environment and our needs change?
- How can you offload day-to-day administrative work from our IT team during and after implementation?

324 days is the average time to detect and contain a data breach caused by a malicious attack on the public sector.[8]

Comprehensive coverage and support

While the profile of emerging threats in state and local governments is concerning, widespread, coordinated network protection coverage can keep you one step ahead of sophisticated and evolving network threats. When you choose security as a managed service, you are supported from design through implementation and ongoing support. Discover how Spectrum Enterprise is uniquely qualified to protect your government's network.

Learn more

1. "The Future State CIO: How the Role Will Drive Innovation," NASCIO, 2020.
2. Ibid.
3. Ibid.
4. David Raths, "In the Shift to Telework, Can We Secure the Virtual Office?" Government Technology, Sept. 20, 2020.
5. "Malware," AV-TEST Institute, accessed Sept. 13, 2021.
6. Renatta Siewert, "Polymorphic Viruses - Best Practices to Prevent Them," June 3, 2021.
7. "SolarWinds Public Sector Cybersecurity Survey Report," SolarWinds, Feb. 21, 2020.
8. "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.

Spectrum ENTERPRISE