▸ GUIDE

Stay a step ahead of cybersecurity threats in government

Spectrum BUSINESS®

Pressure is growing on government organizations to provide easy and convenient digital data access to constituents. At the same time, the increasingly complex systems that serve the public have opened more potential avenues for sophisticated cyberattacks.

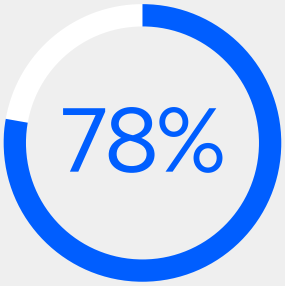
The high value of the data housed on government networks makes them a favored cybersecurity target, and state and local governments find themselves poorly protected compared to their enterprise counterparts in the private sector. Government agencies often face challenges maintaining legacy systems and recruiting cybersecurity experts. Funding difficulties can also hinder security efforts; over half of government agencies cite reducing costs as a top priority through 2030.[1]

The threats targeting state and local governments are constantly evolving. The profiles of distributed denial of service (DDoS) attacks, ransomware and social engineering 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

The profile of threats is concerning. Attacks can lead to expensive breaches that compromise large amounts of sensitive data, while others shut down critical systems and disrupt operations. But you can protect your agency from a wide range of attack vectors. Understanding current and emerging types of threats can help you put the right protection in place.



of state and local IT decision-makers are concerned about AI cybersecurity threats evolving faster than their agency can keep up with.[3]

Social engineering

This technique is used by cybercriminals to exploit human psychology and trick people into revealing confidential information or performing actions that compromise security. Phishing is one common method, with attackers impersonating legitimate entities to steal sensitive data using emails, fake websites or phone calls to deceive government workers. The use of phishing and other social engineering tactics has risen steeply worldwide in recent years.[2]

AI-powered cyberthreats

These emerging methods leverage AI to create more convincing and automated attacks, making them harder to detect and potentially more effective. One example includes using AI to develop deepfakes, which are realistic fake videos, audio or images employed to trick individuals into granting access to systems or data. AI can also help generate highly personalized phishing emails, power chatbot phishing efforts and attack AI systems by corrupting training data or finding vulnerabilities in the models. Approximately 80% of state and local government IT decision-makers are concerned about cyberattacks becoming more sophisticated due to AI, AI systems being manipulated by malicious actors and AI cybersecurity threats evolving faster than their agency can keep up with.[4]

Ransomware and other malware

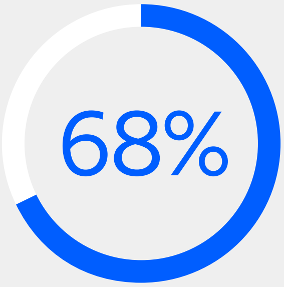
Malware is broadly defined as any malicious software designed to harm or exploit computer systems. Ransomware is a type of malware attackers use to restrict access to a computer system or files and then demand payment for their release. The average ransom demanded from government agencies under attack in 2024 was $2.3 million, with payments to attackers averaging $923,000.[5] Downloaders are another common malware type distributed through malicious or compromised websites, typically via fake software updates. New malware variations appear each year, underscoring the need for organizations to remain up to date and vigilant.

DDoS attacks

These brute-force attacks are throwing more traffic at networks than ever before, combining volumetric, session-exhaustion and application-layer attack vectors. In session-exhaustion attacks, the firewall is essentially turned inside out, becoming a tool for attackers instead of a network defense. Application-layer attacks target the code that runs the website or application. DDoS attacks can be easy for cybercriminals to execute, with subscription attack-for-hire tools available on the dark web for as little as $30 a month.[6]

Data breaches

The unauthorized access, disclosure or loss of sensitive, confidential or protected information continues to be a risk faced by government agencies of all sizes. The theft can involve personally identifiable information (PII), such as Social Security numbers, bank account details and health information. In some cases, attackers prefer to corrupt rather than steal from institutional databases: deleting tables, changing records or erasing entire databases. It's estimated that 1.5 million records were affected by ransomware attacks on government agencies in 2024.[7]



of state governments identify improving data security and privacy measures as a key priority driving updates to the constituent experience.[8]

How cyberattacks can be prevented

Breaking down the details of government cybercrimes helps paint a clear picture of the evolving threat. Read these hypothetical 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 $50,000 in bitcoin to decrypt the data.

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

What might have mitigated or thwarted the attack: Implementing segmented security zones within the network, along with multi-factor authentication (MFA), could have hindered cybercriminals from moving laterally once they gained access to a device. Endpoint security solutions could have helped protect individual devices connected to the network. Use of antivirus software, a next-generation firewall and content scanning and filtering on mail servers could have protected critical data and prevented the intrusion.

Malware infected devices at multiple state agencies

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

What was lost: Agency computers crashed and staff experienced technical issues. Most of the computers that were impacted were PCs with lower processing power.

What might have mitigated or thwarted the attack: The use of a next-generation firewall could have helped block the attack and warned security personnel to act faster. Intrusion detection services, in concert with strong user authentication, could have also protected critical data.

584K

The number of queries per second of the largest DNS query flood attack on a government organization in 2024.[9]

DDoS shut down city and safety services

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

What was lost: The attack rendered both agency 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: Careful monitoring of internet traffic could have detected the attacks. During the attacks, a DDoS mitigation solution could have resulted in blocking only certain IP addresses, allowing clean traffic to pass and productivity to be maintained or restored.

Finding the right protection

Continuously staying ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. A unified security approach integrated with your internet and network connectivity can help you eliminate vulnerabilities and minimize downtime. The approach should include firewalls, unified threat management (UTM) and DDoS protection. The support of a network services provider is also vital, including for cloud-based security services such as secure web gateways, cloud access security brokers, identity management and zero-trust network access.

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

- How can you protect us from malware, phishing and other common cyberattacks?
- How do you identify and mitigate network threats? Can you scan our network for attacks and redirect suspicious traffic?
- What protection do you provide against volumetric DDoS attacks?
- Do you have a means for enabling us to continue to work productively on unaffected parts of the network after a DDoS attack?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic across our various sites?
- Is a next-generation firewall part of what you offer? What does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- Does your solution provide complete visibility across network components to make potential vulnerabilities easier to identify?

- Can you help implement a zero-trust network architecture with MFA, access management and cloud security for staff working on-site and remotely?
- How are you prepared to support our organization as our network needs change and cyberthreats evolve?
- How can you help offload day-to-day administration work from our IT team during and after implementation?
- What types of teams and experts will we have access to for support? Are they available 24/7?
- How will you ensure all of our WiFi sites are protected?

Comprehensive coverage and support

Widespread, coordinated network protection can keep you one step ahead of evolving cyberthreats against state and local governments. You can balance the needs for complexity in coverage and simplicity in operation by choosing managed security services. With the right partner, you're supported from design through implementation and provided with ongoing support. See how Spectrum Business®, a Charter Communications brand, is uniquely qualified to protect your institution's network.

Learn more

1. "EY GPS 2025 Federal Trends Report," EY, 2025.
2. "Global Cybersecurity Outlook 2025," World Economic Forum, January 13, 2025.
3. Suzanne Vitale, "EY Government State and Local 2025 Survey Findings," EY, June 18, 2025.
4. Ibid.
5. Rebecca Moody, "Ransomware Roundup: 2024 End-of-Year Report," Comparitech, January 9, 2025.
6. Michael Hill, "DDoS Attack-for-Hire Services Thriving on Dark Web and Cyber Criminal Forums," Cyber Security Hub, December 4, 2023.
7. Moody, "Ransomware Roundup."
8. "Constituent Experience: State Government IT Strategies," National Association of State Technology Directors, 2025.
9. "2025 Global Threat Analysis Report," Radware, 2025.