ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Improving State and Local Government Cybersecurity

DAVID KERTAI | MAY 2026

State and local governments face rising cybersecurity risks that strain budgets, disrupt services, and erode public trust. Governments need targeted investments in modern infrastructure, continuous monitoring, and stronger third-party risk management to protect critical services.

KEY TAKEAWAYS

- A patchwork of cybersecurity and data protection laws creates conflicting requirements for state and local governments, complicating cross-state collaboration and information sharing.
- State and local governments' dependence on legacy infrastructure complicates and raises costs for adoption of commercial products.
- Minimum product standards and vendor liability would improve resilience, while a unified federal breach-reporting framework would improve coordination and response.
- Cooperative purchasing reduces costs through bulk agreements, while vendor accountability measures would incentivize manufacturers to produce more secure software and hardware.
- Collaborations with universities, nonprofits, and industry deliver affordable, tailored cybersecurity tools and training for all jurisdictions.

CONTENTS

INTRODUCTION

Cyberattacks in the United States have surged in frequency and impact since the start of this decade, with the country facing several hundred on any given day.[1] The proliferation of digital systems and interconnected infrastructure has widened the attack surface, while adversaries have become more organized and technologically advanced, increasing the sophistication of their methods. These trends amplify both the scale and severity of incidents, making recovery costlier and disruptions more prolonged. These attacks strike federal, state, and local governments nationwide regardless of size or location, putting personal data, critical infrastructure, essential government services, and business operations at risk.

State and local governments now stand on the front lines of a rapidly changing cyberspace, facing a range of cyberthreats, from opportunistic attackers exploiting basic security weaknesses to organized groups using advanced techniques. Underfunded IT departments, aging critical infrastructure sectors, and a chronic shortage of cybersecurity professionals leave many state and local governments exposed. At the same time, cybercriminals, organized groups, and nation-state adversaries such as Russia, China, and Iran are deploying increasingly sophisticated tools to exploit these weaknesses. Recent incidents demonstrate the scope of these threats, including the 2023 ransomware attack on Dallas, Texas, which disrupted police, fire, and court systems and exposed 30,000 residents' data; the attack on Oakland, California, that compromised 600 gigabytes of the city's employee data; the 2024 Salt Typhoon infiltration of U.S. telecommunications networks such as Verizon and AT&T; and the 2025 PowerSchool breach that exposed personal information of 62 million students and 9.6 million teachers nationwide, underscoring the scale, persistence, and growing costs of these attacks.[2]

State and local governments now stand on the front lines of a rapidly changing cyberspace, facing a range of cyberthreats, from opportunistic attackers exploiting basic security weaknesses to organized groups using advanced techniques.

This report argues that state and local governments face three key challenges that leave them particularly vulnerable to cyberthreats: the rising costs and frequency of attacks, the growing sophistication of threat actors, and the increasing complexity and interconnectedness of government IT systems. These trends, compounded by chronic resource shortages, fragmented governance structures, and market and regulatory failures, make it increasingly difficult for state and local governments to defend themselves, let alone recover quickly from attacks.

This report then examines the risks and limitations of current approaches, outlines the evolving threat environment, and highlights the systemic gaps in funding, organization, and technology that undermine cybersecurity across the state and local landscapes. It concludes with the following 10 recommendations to secure the essential services on which Americans depend:

1. Make the state and local cybersecurity grant program permanent.
2. Expand the CyberCorps: Scholarship for Service program.
3. Establish regional cybersecurity training hubs.
4. Improve federal, state, and local coordination.

5. Establish state cybersecurity coordination centers.
6. Operationalize the Emergency Management Assistance Compact for cybersecurity missions.
7. Replace ransom payments with dedicated security funding.
8. Set minimum cybersecurity standards for government technology.
9. Adopt strong cybersecurity procurement and reporting standards.
10. Invest in public-sector-tailored cybersecurity tools.

STATE AND LOCAL GOVERNMENTS FACE INCREASED CYBERSECURITY RISK

State and local governments deliver essential services, from elections and emergency response systems to drinking water management and education, making them prime targets for cybercriminals and nation-state actors. Yet, many lack the financial, personnel, and technological resources to implement strong security measures, resulting in mounting vulnerabilities. The widespread adoption of digital technologies, while increasing efficiency and enabling governments to deliver their services in new ways, has also worsened these vulnerabilities by expanding government entities' digital footprints, broadening malicious actors' potential access to their systems and increasing the cost and difficulty of securing them.

Rising costs and expanding digital exposure have enabled cybercriminals and nation-state threat actors to both disrupt services externally and exploit vulnerable systems internally, gaining access for data theft, surveillance, and long-term strike capabilities. This has created an increasingly hostile environment in which under-resourced state and local governments must defend critical infrastructure and services against a growing array of sophisticated threats. Nation-state actors, particularly China, Russia, and Iran, have intensified cyberattacks and espionage campaigns aimed at undermining U.S. capabilities at all levels of government, using persistent, targeted intrusions to steal sensitive data, disrupt government operations, and establish footholds for potential future attacks. As these adversaries continue to exploit systemic weaknesses, the cybersecurity posture of state and local governments has become a critical component of national security.

Rising Costs and Frequency of Attacks

Cyberattacks take many forms, from simple phishing campaigns, in which emails impersonate trusted sources to steal sensitive information, to ransomware, which locks victims out of their data until a ransom is paid, and denial-of-service attacks, which overwhelm a system with traffic to shut it down and potentially allow attackers to circumvent security controls.[3] Threat actors' wide ranging cyber capabilities allow them to cripple a variety of organizations, especially financially limited or burdened ones such as municipal hospitals, public schools, and city governments, by locking up systems and halting essential services for hours, days, or weeks at a time.

Between 2018 and 2024, 525 ransomware attacks targeted federal, state, or local government entities, resulting in an estimated $1.09 billion in downtime.[4] These attacks impose a growing financial burden, forcing governments to cover ransom payments, fund forensic investigations, pay legal fees, and absorb the high costs of restoring systems and securing networks. The

financial impact is especially evident in larger cities, such as Baltimore and Atlanta, which faced ransomware demands of $76,000 and $55,000, respectively. Although neither city paid the ransom, Baltimore spent between $10 million and $18 million, and Atlanta around $17 million, to recover their systems.[5] Some municipalities, however, have opted to pay, and at far higher ransom costs. In 2019, Riviera Beach, Florida, approved a nearly $600,000 ransom payment after an attack crippled its systems, and Lake City, Florida, paid roughly $500,000 in a similar incident.[6] Even cyberattacks without ransom demands can inflict similar costs; according to a 2022 study, the average data breach that year cost $9.36 million, as agencies must still recover compromised systems, restore data integrity, and reassure the public about operational and information security.[7]

Examples from recent years highlight the scale and consequences of these attacks. In 2018, the city of Atlanta spent over $17 million to recover from a ransomware incident that paralyzed court systems, utility billing, and public safety platforms.[8] In 2020, a cyberattack on a Florida water treatment facility attempted to dangerously raise sodium hydroxide levels, a chemical used to regulate water's pH, in the public water supply, raising alarm over critical infrastructure security.[9] In 2021, a breach at the California Department of Motor Vehicles exposed sensitive driver data through a third-party vendor, illustrating how vendor security weaknesses can compromise government systems.[10] In 2022, ransomware struck the Los Angeles Unified School District, disrupting school operations and leaking sensitive student and staff records.[11] In 2023, major attacks hit both Dallas and Oakland, disrupting 911 emergency response, permitting processes, and recordkeeping while stealing terabytes of sensitive data.[12]

Between 2018 and 2024, 525 ransomware attacks targeted federal, state, or local government entities, resulting in an estimated $1.09 billion in downtime.

More recently, the 2024 Salt Typhoon campaign compromised U.S. telecommunications networks.[13] Chinese state-backed actors infiltrated major carriers such as Verizon and AT&T, gaining persistent access to critical systems and remaining dormant until activated. This long-term breach posed a direct threat to public safety, national security, and digital infrastructure.

Cyberattacks continued to accelerate in 2025, both in frequency and in cost. State and local governments are still grappling with the fallout from Salt Typhoon, with new details emerging regularly. A June 11, 2025, Department of Homeland Security (DHS) memo reveals that attackers accessed Army National Guard network diagrams, location maps, and sensitive service member data.[14] Ransomware incidents targeting schools, colleges, and universities have risen 23 percent since January 2025.[15] A major breach at student information system provider PowerSchool leaked personal data for more than 10 million teachers and 60 million students.[16] Beyond these high-profile cases, attacks on smaller municipalities continue on a near-daily basis. In Texas, the cities of Mission and Abilene declared states of emergency and suspended public records access after ransomware incidents, while the Texas Department of Transportation suffered a breach exposing 300,000 crash reports containing medical, insurance, and personal information.[17]

These examples demonstrate that cyberattacks against state and local governments are growing in frequency, scope, scale, and cost. What were once isolated incidents have evolved into

regular, strategically coordinated campaigns that target essential public services, critical infrastructure, and sensitive personal data. From major metropolitan areas to small rural towns, no locality remains immune. The financial burden, from ransom payments to long-term recovery costs, continues to rise, in addition to operational disruption and eroding public trust. As threat actors grow more sophisticated, state and local leaders should confront the rising cost and frequency of cyberattacks as a core governance, public safety, and national security issue.

Evolving Threat Actors

The rising cost and frequency of cyberattacks stems in large part from a widening range of threat actors who increasingly exploit the vulnerabilities in state and local government systems. Financially motivated cybercriminals remain a consistent danger, often deploying ransomware-as-a-service platforms to target schools, hospitals, and municipal agencies.[18] But these actors now operate alongside increasingly sophisticated, well-resourced state-sponsored groups. Nation-state adversaries, especially from China, Russia, and Iran, use cyberoperations not only to cause financial damage but also to gather intelligence, disrupt infrastructure, and maintain long-term system access to pre-position themselves in critical systems they can exploit during future crises or conflicts..[19] State and local governments, with limited resources and weaker cybersecurity postures than federal agencies have, find themselves squarely in the crosshairs of these campaigns.

Modern cyber adversaries frequently employ "living-off-the-land" techniques, leveraging legitimate system administration tools already present in networks to evade detection. Such tactics enable persistent access, bypass traditional antivirus tools, and facilitate lateral movement across systems.[20] State-backed actors also use spear phishing, credential theft, supply chain compromises, and malware-laced software updates to infiltrate targets.[21] Once inside, they may exfiltrate data, map critical infrastructure, or establish dormant access for future disruption. Common practices include exploiting unpatched software, abusing legitimate administrative credentials, targeting cloud services, and compromising third-party vendors.[22] Many operations aim for stealth and persistence rather than immediate damage, positioning the attacker for later espionage, sabotage, and political influence.[23]

Chinese state-backed threat actors have conducted some of the most expansive cyberespionage campaigns against U.S. targets. Often referred to under various "Typhoon" designations, these advanced persistent threat (APT) groups have demonstrated significant scale and capability: Salt Typhoon breached 9 U.S. telecom companies and compromised 200 organizations across 80 countries; Volt Typhoon infiltrated 30 percent of targeted legacy Cisco routers in 37 days while embedding itself in U.S. energy, water, and transportation systems; and Flax Typhoon exploited 66 known vulnerabilities to build a botnet of over 260,000 compromised devices.[24]

More recently, the Salt Typhoon campaign, attributed to China's Ministry of State Security, embedded malware deep in U.S. telecommunications infrastructure, including carriers such as AT&T and Verizon, affecting systems nationwide.[25] The campaign enabled Salt Typhoon to steal 1,462 network configuration files from an estimated 70 U.S. government entities across all levels of government, as well as from 12 critical infrastructure entities, including energy, communications, transportation, and water and wastewater systems.[26] The attack also targeted Army National Guard systems, which could, in the long term, undermine local efforts to protect

critical infrastructure, as National Guard cyberunits play an important role in assisting state and local governments targeted by cyberattacks.

In 2025, Violet and Linen Typhoon exploited Microsoft SharePoint vulnerabilities, impacting hundreds of users and reportedly breaching the Department of Energy and the National Nuclear Security Administration.[27] In addition, this campaign targeted thousands of state and local governments that heavily rely on Microsoft SharePoint. One state official noted that the breach allowed attackers to gain control of a state government website used to publish public-facing documents.[28] CrowdStrike reported that more than 1,100 servers belonging to state and local governments were affected, including servers for public higher education institutions and K-12 schools.[29]

These examples show a clear pattern: Chinese state-backed APT groups are targeting not only high-value federal institutions but also critical infrastructure and network layers that support state and local governments, including telecom carriers, National Guard and emergency response networks, public sector IT systems, and other backbone services. The objective appears to be long-term strategic access, intelligence gathering, and potentially to disrupt or surveil at scale—not just data theft, but structural leverage over local governance and public sector operations.[30]

Chinese state-backed threat actors have conducted some of the most expansive cyberespionage campaigns against U.S. targets.

Russian state-backed threat actors are known for bold, disruptive attacks aimed at undermining election infrastructure and democratic processes.[31] These groups, known under the "Blizzard" designation, including Cozy Bear, Sandworm, and Seashell, operate as arms of Russian intelligence services. Their campaigns often seek to sow distrust, exploit social divisions, and destabilize political institutions.[32] In 2019, Russian operatives breached SolarWinds, a Texas-based IT management firm, inserting malicious code into routine software updates and giving themselves backdoor access to thousands of customers, including U.S. government agencies.[33] The compromise extended beyond federal networks, infiltrating state and local government systems as well as critical infrastructure providers, underscoring the far-reaching consequences of supply chain attacks.[34] The attack ultimately affected more than 18,000 organizations. In 2024, Sandworm, also known as "CyberArmyofRussia_Reborn," attacked water and waste treatment facilities in two smalls towns, Tipton, Indiana, and Muleshoe, Texas, with populations of just over 5,000 each.[35] Although contained, these incidents demonstrate Russia's willingness to target even small municipalities to undermine critical infrastructure, public trust, and national security.

Iranian state-backed actors have likewise expanded their capabilities and ambitions over the past decade. Often grouped under the "Sandstorm" designation, Iranian APTs such as APT33, APT34, APT42, Charming Kitten, and Imperial Kitten conduct aggressive campaigns against U.S. critical infrastructure and government systems.[36] They frequently share malware, stolen credentials, and intrusion techniques to maintain persistent access.[37] Their operations range from spear phishing and credential harvesting to exploiting Internet-connected devices in utilities and transit networks.[38] In 2018, Iranian hackers targeted Atlanta's airport systems.[39] In 2020, they posed as Proud Boys members online in an attempt to intimidate voters during the U.S.

election.[40] In 2023, Iranian-linked attackers breached water utilities in Pennsylvania and Texas by exploiting unpatched Internet of Things devices.[41] Most recently, in 2025, an Iranian-affiliated actor accessed the Arizona Secretary of State's Office and altered candidate profile photos with pictures of Ayatollah Khomeini.[42] While no sensitive data was compromised, this symbolic disruption demonstrated both technical capabilities and Iranian political intent.

Together, these nation-state actors pose a persistent and escalating threat to state and local governments' cybersecurity. Their goals range from long-term intelligence gathering to immediate disruption, but their tactics consistently exploit the public sector's fragmented, underfunded, and outdated cybersecurity infrastructure. As these adversaries continue to evolve and coordinate their attacks, state and local agencies face mounting challenges in defending their systems. Confronting these threats will require not only awareness of their tactics but also a fundamental reassessment of public sector cybersecurity at all levels of government.

Expanded Digital Exposure

The growing costs, frequency of attacks, and evolving number of threat actors stem in part from the continued expansion of digital exposure state and local governments face. The digitalization of governmental and critical infrastructure sectors, from education and energy to water and waste management, has significantly expanded the cyberattack surface. Over the past two and a half decades, state and local entities have increasingly shifted core operations and constituent services online—a shift accelerated rapidly by the transition to remote work and digital service delivery during and after the COVID-19 pandemic.[43] While digital transformation is essential for modern, efficient governance, it has often outpaced cybersecurity investments, leaving many systems exposed.

The COVID-19 pandemic forced rapid technology adoption across government agencies, with many implementing cloud-based platforms, third-party tools, and remote work infrastructure without sufficient risk assessment or long-term planning.[44] This created multiple new attack vectors that threat actors could exploit quickly. For example, during the pandemic, several school districts implemented online learning platforms without robust authentication controls, making them vulnerable to data breaches and ransomware attacks. According to K12 SIX research, a nonprofit specializing in K-12 cybersecurity, cyberattacks rose 393 percent between 2016 and 2022, with incidents ranging from data leaks to system outages that disrupted school operations, which have only increased in frequency since then.[45]

Many state and local agencies still rely on outdated IT infrastructure that lacks essential cybersecurity features such as multifactor authentication, encryption, or real-time monitoring.

The growing reliance on widely adopted software has introduced systemic supply chain risks. The 2023 MOVEit data breach demonstrated how a single vulnerability in commonly used software can cascade across thousands of organizations simultaneously—for instance, a threat actor exploited one flaw in a widely used file transfer tool, exposing sensitive data from over 2,700 organizations, including multiple state agencies.[46] The breach affected state departments of health, education, and motor vehicles, demonstrating how concentration risk, wherein many organizations depend on the same software, can turn a single point of failure into a widespread public sector crisis. Moreover, this incident highlights the growing problem with zero-day

vulnerabilities, which are unknown software flaws discovered only after an incident, that organizations often fail to assess annually, leaving them vulnerable to continuous attacks by various threat actors.[47] Yet, many state and local governments continue to depend on commonly used software and external services without conducting sufficient oversight, establishing contractual security requirements, or having coordinated incident response.

Legacy systems further complicate the picture. Many state and local agencies still rely on outdated IT infrastructure that lacks essential cybersecurity features such as multifactor authentication, encryption, or real-time monitoring.[48] These systems often cannot run modern security software, lack support for current encryption and authentication standards, and are unable to integrate with centralized monitoring tools, making them fundamentally incompatible with today's cybersecurity infrastructure.[49] The combination of aging digital systems and newly adopted digital services creates a fragmented, difficult-to-secure environment. The 2017 WannaCry ransomware attack is a well-known example, wherein threat actors targeted users of an outdated Microsoft Windows operating system, holding hundreds of thousands of individuals' data hostage for ransom.[50] While Microsoft patched this legacy breach, many similarly outdated systems remain in use, raising the possibility for future exploitation by threat actors aiming to access sensitive government data.

In addition to internal vulnerabilities, expanded digital exposure means cybercriminals and state-sponsored groups are increasingly targeting public-facing systems, such as online portals for tax payments, court records, and public health services.[51] In 2023, the city of Fort Worth, Texas, experienced a cyberattack that disrupted its online public records request system, part of a broader trend of targeting local governments' public-facing infrastructure.[52] These seemingly low-risk systems often lack the same protections as more sensitive databases and can serve as entry points for attackers to move deeper into a network.

As state and local governments continue to digitize, the expansion of their online footprint has become both a necessity and a liability. Without dedicated cybersecurity investment and strategic coordination across agencies and jurisdictions, this digital exposure will remain a major driver of vulnerability and a growing invitation for exploitation by increasingly sophisticated adversaries.

STATE AND LOCAL GOVERNMENT CYBERSECURITY IS FRAGMENTED, UNDERFUNDED, AND UNPREPARED

Despite mounting threats and rising costs from cyberattacks, state and local governments remain chronically underprepared to defend their digital infrastructure. The scale and complexity of modern cyberthreats have outpaced the resources, staffing, and organizational structures available to most public sector entities below the federal level. While some larger jurisdictions have modernized their cybersecurity programs, the overall landscape is fragmented across budgets, capabilities, municipalities, and levels of responsibility.

Many state and local agencies operate with outdated technology, overextended information-technology teams, and limited access to specialized cybersecurity expertise. This disparity is especially severe in rural areas and small municipalities, where basic security practices such as multifactor authentication, endpoint detection, and employee cyber hygiene training may be missing altogether. The result is a patchwork of cyber readiness across the country, with smaller

agencies remaining especially vulnerable to increasingly sophisticated threat actors and lacking the capacity to respond quickly or coordinate with federal partners during attacks.

Beyond resource constraints, systemic issues related to governance, market dynamics, and regulatory oversight have hindered state and local governments' efforts to modernize. Disjointed procurement processes, overlapping agency responsibilities, unclear reporting requirements, and limited access to affordable, tailored cybersecurity solutions compound the problem.

Resource and Capacity Limitations

State and local governments consistently face significant resource and capacity constraints that impede the implementation and maintenance of effective cybersecurity programs. Many agencies operate with understaffed teams, aging infrastructure, and weak or reactive incident response systems. These limitations leave governments dangerously exposed to cyber adversaries capable of crippling essential services, stealing sensitive data, and eroding public trust. The Government Accountability Office has also documented how capacity shortfalls—such as insufficient staffing and outdated technology—undermine the ability of cybersecurity programs to sustain operations and keep pace with evolving threats.[53]

State and local governments operate with limited and often inconsistent cybersecurity budgets, relying heavily on fragmented sources such as short-term grants, appropriations, or redirected operational funds. A critical funding source is the State and Local Cybersecurity Grant Program (SLCGP) administered by Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA); however, its future remains uncertain, as the most recent extension funds the program only through the end of fiscal year 2026, creating a real risk of expiration if policymakers fail to reach a long-term agreement.[54] State and municipal leaders warn that without predictable federal support, long-term planning, infrastructure modernization, and timely response to emerging cyberthreats will remain challenging.[55] Many agencies lack a dedicated cybersecurity budget, forcing IT departments to juggle basic operations with threat response, an unsustainable trade-off as attacks become more frequent and severe.

The United States faces a gap of approximately 500,000–700,000 unfilled cybersecurity roles, according to the National Institute of Standards and Technology (NIST) and private estimates.

Still, designing and executing sustainable solutions requires acknowledging the structural pitfalls that have hindered past efforts. First, administrative burdens frequently overwhelm small jurisdictions: the time and personnel required to apply for, manage, and report on grant programs can drain capacity from frontline defense, leading some agencies to underutilize available funds.[56] Second, inefficiency and duplication persist across programs. Without clear prioritization and coordination, jurisdictions may build overlapping capabilities or adopt one-size-fits-all solutions that fail to meet local needs.[57] For example, Pennsylvania found that before it established shared services and solutions, each of its 67 counties had independently built its own security services and measures, duplicating efforts, exhausting resources, and increasing costs and complexity across the state.[58] These systemic challenges dilute the impact of limited resources and make it harder for governments to build lasting, scalable cybersecurity capacity.

Moreover, DHS's fiscal year 2025 guidance for the SLCGP introduced major changes, limiting how state and local governments can use federal funds. Notably, grant funding can no longer cover memberships to the Multi-State Information Sharing and Analysis Center (MS-ISAC) or the Elections Infrastructure ISAC (EI-ISAC), both operated by the Center for Internet Security (CIS).[59] These organizations have long provided critical, federally funded cyberthreat intelligence and incident response services to state and local governments. At the same time, the pending expiration of DHS's contract with CIS may end federal support that has historically allowed CIS to offer these services free of charge.[60]

To adapt, CIS has introduced a subscription-based model with discounted options, including deferred billing, half-price memberships, and free access for some small jurisdictions.[61] While intended to ease the transition, this shift raises concerns about financial sustainability for both small, underserved local governments and CIS itself. Many smaller entities may be unable to afford even discounted rates, and reduced federal funding could limit CIS's ability to maintain high-quality, up-to-date threat intelligence. These changes threaten the future of multistate cyber coordination, particularly for communities most dependent on federally subsidized support.

The cybersecurity workforce shortage further exacerbates this challenge. The United States faces a gap of approximately 500,000–700,000 unfilled cybersecurity roles, according to the National Institute of Standards and Technology (NIST) and private estimates.[62] Public sector agencies, especially at the state and local levels, struggle to recruit and retain talent, competing with the private sector's higher salaries and more dynamic work environments.[63] Even major state governments often lack teams with specialized skills in threat intelligence, incident response, or vulnerability management, relying instead on generalist IT staff without deep security expertise.[64]

These personnel and financial challenges are compounded by outdated infrastructure. Many agencies still rely on legacy systems, some decades old, that are expensive to maintain, unsupported, and incompatible with modern cybersecurity tools.[65] Such platforms introduce known vulnerabilities and limit secure modernization efforts. To compensate, many agencies outsource critical functions such as cloud hosting, threat monitoring, and application development to third-party vendors.[66] While outsourcing may offer short-term relief, it also introduces risks related to vendor oversight, data security, and supply chain vulnerabilities.

Organizational and Structural Weaknesses

A major organizational barrier to stronger cybersecurity at the state and local levels is inconsistent security practice across agencies and jurisdictions. Individual agencies typically remain responsible for their own cybersecurity, but without common standards, shared threat intelligence, or coordinated response capabilities, security maturity varies widely. Some agencies implement robust controls, while others lack basic protections such as multifactor authentication or regular patching. States have created chief information security officer positions or centralized IT agencies, but their authority often only extends to executive branch agencies, leaving local governments and other departments to develop their own security approaches. Without mechanisms to share practices and coordinate responses, agencies operate in silos, slowing threat responses and undermining resource allocation efforts.

The misalignment of priorities between federal, state, and local governments further complicates cohesive cybersecurity responses. At the federal level, agencies concentrate on large-scale, high-impact threats, such as infrastructure sabotage, due to these risks carrying national security

implications and require centralized coordination and response. State and local entities, however, operate in a different environment, frequently facing threats such as ransomware that shuts down schools and city services, business email compromise schemes, and data breaches that expose citizens' information.[67] This disconnect between levels of government is a natural result of each government's differing priorities; however, federal strategy should still remain attentive to operational realities and resource constraints of state and local entities.[68] When this awareness is lacking, it creates gaps in support, funding mismatches, and fragmented access to federal threat intelligence and resources, leaving state and local jurisdictions without the federal assistance needed to address the cyber risks they encounter most frequently.[69]

A fragmented security posture across jurisdictions amplifies these weaknesses. Cybersecurity capabilities vary significantly from one locality to another, depending on leadership, budgets, and organizational capabilities. Some agencies have deployed advanced defenses and applied strong cyber-hygiene protocols, while others operate with minimal safeguards, sometimes lacking even basic protections such as multifactor authentication or regular patching. These inconsistencies create security vulnerabilities that attacks can exploit, moving from less protected points to access more sensitive systems, while also reducing opportunities for scaling defenses through shared services or bulk contracting.[70] With disparate systems and practices across agencies, sharing threat intelligence and learning from each other's incidents become much more difficult, leaving jurisdictions to face the same attacks repeatedly without collective defense.

Moreover, unclear roles and responsibilities during a cyber incident frequently hinder effective response and recovery. In many states, it remains ambiguous which agency should lead a response involving multiple localities or outside vendors. Without well-established incident frameworks that include all levels of government, local emergency managers, and public information officers, responses can be delayed, mis-coordinated, or redundant.[71] The absence of both rehearsed protocols and clarity on leadership during a cyber crisis further undermines the public sector's capacity to respond to fast-moving threats.

Together, these structural weaknesses, fragmented oversight, misaligned priorities, inconsistent security postures, and unclear incident leadership limit the ability of state and local governments to build resilient cybersecurity defenses. Even jurisdictions with adequate funding may struggle to defend against today's evolving threats without greater clarity, coordination, and cohesion across agencies and levels of government.

Market, Technology, and Regulatory Failures

Many tools and technologies deployed by state and local governments lack built-in security features. Particularly in operational technologies—the control systems that run water treatment facilities, electric grids, and transportation network—products used in utilities and infrastructure frequently reach operators without modern security controls, leaving them vulnerable the moment they are deployed. A recent review of 45 operational technology product families finds that every system has at least one trivial but exploitable security flaw, such as lack of encryption or the ability to execute arbitrary code without constraints.[72] Default configurations may ship with shared passwords or exposed administrative ports, and procurement policies at state and local levels are often insufficient to prevent insecure products from entering public systems.

The hurdles in this area are multifaceted. The first challenge is the widespread use of insecure commercial products, which often ship with weak default configurations that expose agencies to

compromise before deployment. A second challenge is that purchasing decisions are frequently driven by short-term costs or convenience rather than security, resulting in systems that introduce long-term risk as well as the associated long-term costs from these risks.[73] A third obstacle is the lack of vendor accountability, as many contracts lack enforceable security requirements and provide few consequences for undisclosed vulnerabilities or delayed patches.[74] Finally, compliance burdens compound these issue. States and local agencies have to navigate sector-specific federal regulations—such as the Health Insurance Portability and Accountability Act (HIPAA) for health departments, the Family Education Rights and Privacy Act (FERPA) for schools, and Criminal Justice Information Services—each imposing technical obligations that strain limited resources and cause small agencies to divert staff from practical defense to documentation and audit tasks.[75] Even aligning with national frameworks such as NIST or CISA proves difficult when small jurisdictions lack the budget and staff these guidelines require.

While some jurisdictions have adopted cybersecurity procurement checklists, they remain inconsistent and rarely comprehensive. Often, cost, speed, or familiarity drives decision-making over security. CISA's Software Acquisition Guide strongly recommends formal documentation of risks and executive sign-off when considering insecure products, yet few agencies consistently follow these protocols.[76] Case studies reveal that procurement processes focused on price over security result in long-term vulnerabilities and increased exposure.[77]

A lack of vendor accountability exacerbates these weaknesses. Many contracts lack enforceable security requirements, and governments rarely hold vendors liable for undisclosed vulnerabilities. Some vendors delay or overlook post-deployment patches or fixes, and smaller agencies lack the leverage to demand rapid response and secure-by-design products. As a result, cybersecurity responsibility falls disproportionately on under-resourced government buyers that are often unprepared for these tasks.

Commercial cybersecurity tools and services frequently do not meet public sector needs. Many are built for enterprise customers with large IT teams, big budgets, and modern infrastructure, making them misaligned with government procurement rules and difficult to integrate with legacy systems. Smaller agencies often either overpay for unnecessary features or find themselves unable to adopt usable tools due to technical complexity or incompatibility.[78] This misalignment reinforces the digital divide between well-funded and under-resourced jurisdictions, leaving the latter exposed despite available, but ill-fitting, solutions.

Even when awareness exists, many state and local governments deprioritize cybersecurity in budgeting and policy decisions. Departments frequently treat security as an IT issue rather than a core operational risk, delaying or minimizing long-term investments in technology and staffing. Studies from industry experts confirm that budget constraints and competing priorities continue to sideline cybersecurity in many local government settings.[79] The result is lower readiness and reduced ability to mitigate or recover from attacks, leading to higher overall impact.

At the regulatory level, a patchwork of state-specific data protection and cybersecurity laws adds complexity for multijurisdictional agencies and vendors. Compliance requirements vary widely across states and often conflict, creating barriers to cooperation and increasing procurement costs. Aligning with federal frameworks, such as NIST or CISA guidance, can be difficult for local governments that need to tailor solutions to local operational needs and budgets.[80] These inconsistencies limit scalability, increase overhead, and strain already limited resources.

Table 1: Unique cybersecurity challenges facing state and local governments

Challenge	State & Local	Federal	Private Sector
Increasing cyberattacks	✓	✓	✓
Expanding digital exposure	✓	✓	✓
Workforce shortages	✓	✓	✓
Third-party/vendor risks	✓	✓	✓
Nation-state threats	✓	✓	✓
Coordination	✓	✓	
Misaligned priorities	✓	✓	
Fragmented intelligence sharing	✓	✓	
Nation-state targeting	✓	✓	
Inconsistent standards	✓	✓	
Supply chain vulnerabilities		✓	✓
Protecting critical infrastructure		✓	✓
Need secure-by-design technology		✓	✓
Responsibility for cloud/telecom security		✓	✓
Legacy systems and integration issues	✓		✓
High cost of cyber incidents	✓		✓
Difficulty maintaining secure configurations	✓		✓
Heavy reliance on vendors	✓		✓
Limited funding	✓		
Small cybersecurity workforce	✓		
Outdated systems	✓		
Frequent ransomware attacks	✓		
Focus on national threats		✓	
Complex agency coordination		✓	
Slow intelligence sharing		✓	
Constant need for updates/patches			✓
Entry point for attacks on others			✓
Pressure to move quickly, not securely			✓
Vulnerable supply chains			✓
High financial risk from attacks			✓

RECOMMENDATIONS

Cybersecurity at the state and local levels should be treated as a governance priority, not merely an IT function. Solutions should prioritize longevity, adaptability, and capacity-building. Short-lived pilot programs, grants, and narrowly scoped projects cannot keep pace with the rapidly-evolving capabilities of increasingly persistent, innovative, and well-resourced adversaries. State and local governments need sustained funding mechanisms, strong workforce pipelines, scalable technologies, and clearly defined lines of coordination between all government-level actors and agencies. Withstanding today's threats and those to come requires not only building strong collaboration between government entities, but also strengthening partnerships with private sector suppliers and civil society.

The recommendations that follow address these needs across three structural categories: the resource and capacity limitations that constrain day-to-day cybersecurity operations; the organizational and governance weaknesses that hinder coordination and consistency; and the market, technology, and regulatory failures that allow insecure products and fragmented rules to persist. Together, these reforms outline a comprehensive approach to embedding cybersecurity into the fabric of basic governance. Achieving this vision requires federal leadership and coordinated action across all levels of government to ensure cybersecurity functions as an essential public service.

Resource and Capacity Limitations

State and local governments are unique not because the threats they face are uniquely severe, but because their ability to respond is chronically under-resourced. Even as cyberattacks grow more frequent, costly, and sophisticated, many jurisdictions operate with aging infrastructure, understaffed IT teams, and fluctuating budgets.[81] These constraints create a structural disadvantage wherein governments are expected to defend increasingly complex digital environments with tools, personnel, and funding models that were never designed for today's threat landscape.

The result is a widening gap between what state and local agencies must secure and what they can realistically support. Short-term grants, fragmented training pipelines, and limited access to specialized expertise leave many jurisdictions reliant on temporary fixes rather than long-term resilience.[82] Without stable funding, sustainable workforce development, and shared regional capacity, even well-intentioned agencies struggle to modernize systems, adopt secure-by-design technologies, or maintain consistent cyber readiness—highlighting the need for long-term federal funding, expanded talent pipelines, and scalable regional training and support programs.

1. Make the State and Local Cybersecurity Grant Program Permanent

Among the most significant barriers to stronger cybersecurity at the state and local levels are the resource and capacity constraints. Congress should make the SLCGP permanent with consistent annual appropriations.[83] Congress has reauthorized the program through September 2026, but without providing new funding, thereby ending existing grant opportunities. The Protecting Information by Local Leaders for Agency Resilience (PILLAR) Act would extend the program through 2033 with additional funding.[84] A consistent funding stream would shift agencies away from chasing short-term patches toward long-term strategy.[85] Permanent funding would enable jurisdictions to prioritize cost-effective security investments, such as secure-by-design products and vendor accountability measures, rather than repeatedly patching vulnerable systems,

allowing governments to invest in architecture modernization and hire permanent cybersecurity staff without fearing that support might vanish mid-cycle. Stable funding would also help jurisdictions maintain momentum across elections or leadership cycles rather than suffer resets.

2. Expand the CyberCorps: Scholarship for Service Program

Congress should expand the CyberCorps: Scholarship for Service (SFS) program to include a buy-in option for state and local government placements. The SFS program currently funds cybersecurity education in exchange for service in qualified government positions.[86] The National Science Foundation should amend the program's authorization to establish explicit buy-in pathways that would allow state and local agencies to directly sponsor and recruit SFS graduates.[87] By enabling state and local government buy-ins, the program could channel more talent into areas with the most acute need rather than concentrating placements only at the federal level. Local governments could gain access to highly trained personnel without bearing the entire recruitment burden, while scholarship recipients would gain opportunities to serve throughout various levels of government, learning a whole-of-country approach about the state of cybersecurity.

3. Establish Regional Cybersecurity Training Hubs

At the state and local levels, workforce initiatives are also key to amplifying federal support. Regional cybersecurity training hubs, developed in partnership with public universities and community colleges, can provide scalable training in simulated network environments wherein students practice detecting and responding to cyberattacks in safe, controlled settings, and technical certification pathways. These hubs reduce overhead for small jurisdictions by pooling resources while delivering consistent, high-quality instruction.[88] In parallel, cyber apprenticeship and reskilling programs, targeted at veterans, displaced workers, and other nontraditional talent pools, can fill critical staffing gaps. Apprenticeship models could combine classroom instruction with hands-on experience, allowing participants to contribute immediately while ramping up proficiency. Expanding pipelines beyond a four-year degree accelerates hiring flexibility and increases diversity in the cybersecurity workforce.

A proof of concept for these ideas is embodied in the 2025 establishment of Texas Cyber Command, signed into law by Governor Greg Abbott. The Cyber Command consolidates cybersecurity responsibilities for state, local, and educational institutions under one coordinating entity based in San Antonio.[89] It includes a threat intelligence center, digital forensics lab, and incident response units, and offers shared services, such as training and incident support, to smaller jurisdictions. By centralizing functions and reliably funding operations, Texas demonstrates how a stable backbone organization can scale capacity, relieve burdens on individual agencies, and incentivize coordination across the public sector.

Together, these measures offer a roadmap for fundamentally reshaping state and local cybersecurity postures. Federal action should deliver predictable funding and expand talent pipelines, while state and local programs should build practical training frameworks and real-world pathways into cybersecurity careers. These recommendations directly address sustainability, administrative complexity, and scalability; when properly aligned and implemented, they will empower even smaller or under-resourced jurisdictions to defend themselves, manage risk proactively, and reduce the cascading costs of cyber incidents.

Organizational and Structural Weaknesses

State and local governments face inconsistent security standards and policies across jurisdictions, combined with limited capacity to scale effective protections. As cyberthreats grow more sophisticated, targeting a widening array of digitalized systems, governments are under pressure to adapt quickly. Stronger cybersecurity structures should prioritize resource efficiency, inter-agency collaboration, and shared tools and services to ensure that security investments deliver maximum value. Without such reform, responses will remain uncoordinated, leaving smaller jurisdictions at heightened risk and undermining national resilience.

However, several hurdles complicate progress. While the federal government has spent decades building robust public-private partnerships and can leverage these relationships and dedicated resources to prepare effectively, state and local entities cannot.[90] Service delivery at the state and local levels is uneven. Some larger states and metropolitan governments have the funding and personnel to implement strong cyberdefenses, but many still struggle, especially rural or underserved communities, which remain particularly vulnerable.[91] Shared services would help address these disparities. States should establish voluntary threat intelligence sharing, facilitate cooperative purchasing agreements for security tools, or provide regional incident response teams that offer surge capacity during major breachers. Such approaches enable resource sharing and coordination, while allowing agencies to maintain autonomy over their core priorities.

4. Improve Federal, State, and Local Coordination

At the federal level, multiple reforms could improve coordination and oversight. Creating dedicated state and local liaison offices would streamline access to federal resources, such as CISA services, while helping agencies navigate assistance programs more effectively.[92] Expanding joint cyber exercises with private sector operators in sectors such as energy, transportation, and healthcare would also strengthen cross-sector preparedness. The Joint Ransomware Task Force, co-led by the Federal Bureau of Investigation, Secret Service, and CISA, should address documented coordination gaps by establishing formal procedures for ransomware assistance to state and local governments, improving consistency in FBI communication during incidents, and clarifying federal agency roles to prevent duplicative efforts and wasted resources.[93]

5. Establish State Cybersecurity Coordination Centers

At the state and local levels, governments should take complementary steps. Establishing state cybersecurity coordination centers would connect local agencies to existing federal Information Sharing and Analysis centers, ensuring that smaller jurisdictions receive actionable information.[94] States should also conduct joint cyber exercises tailored to local contexts, involving hospitals, election offices, and utilities to ensure readiness across the public–private ecosystem. Most importantly, states should create cybersecurity coordination offices to facilitate threat intelligence sharing, harmonize incident response across agencies, and serve as the states' primary liaisons to federal partners.[95]

6. Operationalize the Emergency Management Assistance Compact for Cybersecurity Missions

To further strengthen interstate support during major cyber incidents, the National Governors Association should operationalize the Emergency Management Assistance Compact (EMAC)—a mutual aid framework that allows governors to request personnel and resources from other states

during emergencies—for cybersecurity missions.[96] This should include supporting the development of cyber-specific Mission Ready Packages and clarifying legal, administrative, and reimbursement pathways for deploying cyber personnel across state lines. These steps would allow states to rapidly surge qualified analysts, incident responders, and technical teams during large-scale cyberattacks.

Case studies show that these recommendations are both politically feasible and operationally effective. In 2025, Texas established the Texas Cyber Command, consolidating cybersecurity functions across state, local, and higher-education institutions. With $135 million in dedicated funding, the command now provides shared intelligence, forensics, and incident response services to smaller jurisdictions, reducing duplication and ensuring consistent coverage across the state.[97] New York's 2025 cybersecurity law offers a different but complementary model. It mandates annual cyber awareness training for all state and local employees and requires agencies to report incidents within 72 hours.[98]

7. Replace Ransom Payments With Dedicated Security Funding

While state and local governments gain valuable insight into ransomware trends when victims report payments, allowing those payments to continue ultimately sustains the threat. A coordinated ban across jurisdictions would remove the profit motive that drives these attacks, making them less attractive and likely reducing their frequency over time.[99] States such as North Carolina and Florida have already enacted ransom payment bans, and states pursuing similar legislation should pair prohibitions with dedicated cybersecurity enhancement funds to help smaller jurisdictions upgrade security systems and implement backup solutions before bans take effect.[100]

By combining federal reforms with state-level innovation, governments can overcome hurdles impeding effective cybersecurity measures. A stronger organizational and structural foundation would ensure not only that resources are better utilized, but also that every jurisdiction, from large cities to small towns, has access to the tools and support needed to withstand cyberthreats. Ultimately, building these structures is essential to moving from today's fragmented, reactive posture toward a cohesive, scalable, and resilient national cyberdefense system.

Market, Technology, and Regulatory Failures

Even with stronger resources and organizational structures, state and local governments face systemic disadvantages rooted in the tools they use, the markets they operate in, and the regulatory environment they must navigate.

The New York 2025 cybersecurity law provides a concrete model for addressing these challenges. By mandating annual cybersecurity training and requiring agencies to report incidents within 72 hours, New York established a consistent baseline across state and local agencies.[101] The state provides free training through the Office of Information Technology Services, though it does not fund broader security improvements that smaller jurisdictions need in order to meet these requirements. These measures directly address procurement and vendor accountability: standardized training improves oversight of technology purchases, while disclosure requirements create pressure for vendors to maintain secure systems and respond quickly to vulnerabilities. This kind of model law reduces fragmentation, creates uniform expectations, and strengthens both government and vendor accountability.

Other states should adopt this approach to ensure consistent procurement standards, enforceable reporting rules, and streamlined oversight across the public sector.[102] However, states should also improve New York's model by pairing these reporting measures with dedicated cybersecurity funding, such as upgrading legacy systems, purchasing endpoint protection tools, implementing multifactor authentication, and hiring specialized cybersecurity staff to meet these new requirements.[103]

8. Set Minimum Cybersecurity Standards for Government Technology

At the federal level, policymakers should adopt complementary measures to close systemic gaps. First, federal agencies should establish minimum cybersecurity requirements for all technology products purchased with federal or federally supported funds, ensuring that insecure-by-design systems never enter government networks. Second, Congress should enact legislation on vendor accountability, mandating timely vulnerability disclosure and enforceable cybersecurity obligations in contracts. Doing so would shift risk back onto providers rather than under-resourced government buyers. Third, CISA should expand its procurement guidance and risk assessment tools, offering standardized checklists, model contract language, and technical assistance to help governments prioritize security in purchasing decisions.[104] Finally, to eliminate compliance inefficiencies, Congress should establish a federal framework for breach reporting and data protection, preempting conflicting state rules. A single standard would simplify compliance for vendors and agencies alike while ensuring faster, more consistent reporting of incidents.

9. Adopt Strong Cybersecurity Procurement and Reporting Standards

State and local governments also have critical roles to play. They should adopt cybersecurity procurement standards that evaluate vendors' patch management practices, security certifications, and adherence to secure-by-design principles. Joint procurement agreements could strengthen bargaining power, reduce costs, and improve product quality, while vendor accountability frameworks, such as requiring cybersecurity insurance or guaranteed patch timelines, would shift responsibility away from vulnerable jurisdictions. The New York law underscores how codified training and reporting mandates can institutionalize protections, ensuring that agencies don't rely solely on procurement officers to enforce security.[105]

10. Invest in Public Sector Tailored Cybersecurity Tools

States should also invest in public-sector–tailored tools. Many commercial cybersecurity products are built for large enterprises, making them expensive, overly complex, or incompatible with government legacy systems. By partnering with universities, nonprofits, and industry consortia, states could foster the development of affordable, user-friendly solutions designed for local governments. Regulatory alignment is equally important: States can harmonize their cybersecurity and data protection laws with federal frameworks and neighboring jurisdictions, reducing duplication and making compliance more achievable for small agencies.

Together, these reforms would help governments overcome systemic disadvantages created by insecure products, weak procurement practices, and fragmented regulation. Federal action can establish secure baselines and hold vendors accountable, while state and local initiatives can strengthen procurement practices, create bargaining leverage, and develop tools aligned with public needs. By drawing on frameworks such as New York's 2025 law, policymakers can set consistent expectations, simplify compliance, and institutionalize accountability. Taken together,

these measures would enable governments to not only secure their own systems, but also contribute to a more resilient digital ecosystem across the public sector.

CONCLUSION

State and local governments stand at the front line of a cyberthreat landscape that is growing more complex, costly, and disruptive with each passing year. The very systems that communities rely on daily—emergency services, schools, utilities, and election infrastructure—are increasingly vulnerable to ransomware, data breaches, and sophisticated nation-state campaigns. Unlike the federal government, which benefits from an array of dedicated cybersecurity agencies, state and local entities often face these challenges with fragmented structures, outdated tools, and limited capacities. The result is a widening gap between the scale of threats and the ability of public institutions to defend against them.

This report underscores that these risks are not hypothetical. Recent attacks on cities such as Dallas and Oakland, the 2024 Salt Typhoon infiltration of telecommunications networks, and the 2025 PowerSchool breach demonstrate how quickly local disruptions can escalate into national security concerns.[106] Nationwide surges in cyberattacks have caused hospitals to delay surgeries, schools to suspend classes, and cities to shutter essential services, underscoring that the stakes are no longer only financial and that these attacks are increasingly affecting civil security. Adversaries ranging from cybercriminal groups to state-backed actors in China, Russia, and Iran are deliberately targeting the weakest points of America's cyberdefenses, exploiting underprepared agencies to gain footholds across U.S. critical infrastructure.[107] Without decisive action, these incidents will only increase in frequency, impact, and size.

However, the challenges outlined in this report are not insurmountable. By addressing resource and capacity limitations, strengthening organizational and structural frameworks, and reforming market and regulatory environments, governments at every level can take meaningful steps toward greater resilience. Making federal funding streams permanent, building a sustainable workforce pipeline, clarifying lines of authority, and holding vendors accountable for secure-by-design practices are not just policy options; they are also necessary foundations for defending public services in the digital age. This reality makes investment in cybersecurity not only a simply technical matter, but also a governance, resilience, and national security imperative. Solutions should be scalable, sustainable, and collaborative, ensuring that even the smallest municipality can benefit from shared knowledge, pooled resources, and national coordination.

The stakes are high; cybersecurity is no longer a niche technical issue but rather a fundamental challenge to national security and public trust. Protecting communities from disruption requires a whole-of-country approach that empowers state and local entities as full partners in defense. Ultimately, strengthening state and local cybersecurity is about more than networks. It is about preserving democratic institutions, ensuring resilient infrastructure, and safeguarding the safety and well-being of the American people.

About the Author

David Kertai is a research assistant specializing in cybersecurity at ITIF. He holds a B.A. in European studies and French from the University of Washington and is pursuing a master's degree in security policy studies at George Washington University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. "How many cyberattacks occur in the U.S.?" USAFacts, last modified October 21, 2025, https://usafacts.org/articles/how-many-cyber-attacks-occur-in-the-us.
2. Darwin BondGraham, "Hackers leaked a second, larger set of stolen city files on the dark web," *The Oaklandside*, April 5, 2023, https://oaklandside.org/2023/04/05/ransomware-attack-hackers-oakland-second-data-leak-confidential-city-files; Jonathan Greig, "Cyber incidents in Texas, Tennessee and Indiana impacting critical government services," *The Record*, October 22, 2025, https://therecord.media/cyber-incidents-texas-tennessee-indiana; Tim Starks, "Salt Typhoon hacking campaign goes beyond previously disclosed targets, world cyber agencies say," *CyberScoop*, August 27, 2025, https://cyberscoop.com/salt-typhoon-hacking-campaign-goes-beyond-previously-disclosed-targets-world-cyber-agencies-say.
3. "Type of Cyber Attacks," Fortinet, accessed October 10, 2025, https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks.
4. Paul Bischoff, "Ransomware attacks on US government organizations have cost over $1.09 billion," Comparitech, March 18, 2025, https://www.comparitech.com/blog/information-security/government-ransomware-attacks.
5. "The Economic Impact of Cyber Attacks on Municipalities," KnowBe4, accessed December 1, 2025, https://openapproach.com/wp-content/uploads/2022/09/Economic_Impact_of_Cyber_Attacks_on_Municipalities.pdf.
6. Benjamin Freed, "Florida city pays hackers $600,000 after ransomware attack," *StateScoop*, June 20, 2019, https://statescoop.com/florida-city-pays-hackers-600000-after-ransomware-attack; Andrew Caplan, "Lake City, Fla., Authorizes Nearly $500K Ransomware Payment," Government Technology, June 26, 2019, https://www.govtech.com/security/lake-city-fla-authorizes-nearly-500k-ransomware-payment.html.
7. "The High Cost of Doing Nothing: How Legacy Systems Leave Government's Exposed," Springbook, accessed November 22, 2025, https://springbrooksoftware.com/the-high-cost-of-doing-nothing-how-legacy-systems-leave-governments-exposed-outdated-software-cybersecurity.
8. Kelli Young, "Cyber Case Study: City of Atlanta Ransomware Incident," Coverlink Insurance, September 20, 2021, https://coverlink.com/case-study/city-of-atlanta-ransomware.
9. Andy Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," *WIRED*, February 8, 2021, https://www.wired.com/story/oldsmar-florida-water-utility-hack/.

10. Linda Rosencrance, "5 biggest risks of using third-party service providers," *CSO*, June 21, 2024, https://www.csoonline.com/article/574543/5-major-risks-third-party-services-may-bring-along-with-them.html.
11. Joshua Bote, "California DMV hit by data breach, exposing millions of drivers' personal information to hackers," *SFGate*, February 18, 2021, https://www.sfgate.com/bayarea/article/California-DMV-hit-data-breach-ransomware-attack-15959944.php.
12. Everton Baily, Jr., "Federal agency investigating Dallas ransomware attack; number affected up to 30,253," *The Dallas Morning News*, August 17, 2023, https://www.dallasnews.com/news/politics/2023/08/17/federal-agency-investigating-dallas-ransomware-attack-number-impacted-up-to-30253; Ricky Rodas, "Ransomware attack causes Oakland to declare local state of emergency," *The Oaklandside*, February 15, 2023, https://oaklandside.org/2023/02/15/ransomware-attack-causes-oakland-to-declare-local-state-of-emergency.
13. Chris Jaikaran, "Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications," Congressional Research Service, January 23, 2025, https://www.congress.gov/crs-product/IF12798.
14. David Dimolfetta, "Salt Typhoon hack into National Guard systems a 'serious escalation', experts warn," *Nextgov FCW*, July 16, 2025, https://www.nextgov.com/cybersecurity/2025/07/salt-typhoon-hacks-national-guard-systems-serious-escalation-experts-warn/406765/.
15. Rebecca Moody, "Ransomware Roundup: H1 2025 stats on attacks, ransoms, and active gangs," Comparitech, July 2, 2025, https://www.comparitech.com/news/ransomware-roundup-h1-2025.
16. Briana Mendez-Padilla, "Ransomware attacks in education jump 23% year over year," *K-12 Dive*, July 21, 2025, https://www.k12dive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/753483.
17. Jonathan Greig, "Texas city takes systems offline after cyberattack," *The Record*, April 21, 2025, https://therecord.media/texas-abilene-offline-cyberattack-systems; Sophia Fox-Sowell, "Mission, Texas, requested state of emergency after cyberattack. Some analysts aren't so sure," *StateScoop*, March 14, 2025, https://statescoop.com/mission-texas-state-emergency-cyberattack-2025.
18. Alex Scroxton, "Financially motivated cyber crime remains biggest threat source," *Computer Weekly*, April 23, 2025, https://www.computerweekly.com/news/366623134/Financially-motivated-cyber-crime-remains-biggest-threat-source.
19. "Nation-State Threats," CISA, accessed September 10, 2025, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.
20. "Identifying and Mitigating Living Off the Land Techniques," National Security Agency, February 7, 2024, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combatting-cyber-threat-actors-perpetrating-living-off-the-land-intrusions.
21. "Type of Cyber Attacks," Fortinet.
22. "NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations," CISA, October 5, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a.
23. Feyisayo Mariam Yussuf, "Advanced Persistent Threats (APTs) and U.S. National Security: A Multi-Layered Defense Strategy," *Journal of Computer Engineering*, March 27, 2025, https://www.iosrjournals.org/iosr-jce/papers/Vol27-issue2/Ser-2/G2702023857.pdf.
24. A. J. Vicens, "US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage," *Reuters*, December 27, 2024, https://www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27; "Threat Intelligence Research: Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days," Security Scorecard, January 11, 2024, https://securityscorecard.com/blog/threat-intelligence-

research-volt-typhoon; David Jones, "CISA catalog falls short on CVEs targeted by Flax Typhoon," Cybersecurity Dive, September 24, 2024, https://www.cybersecuritydive.com/news/vulnerabilities-flax-typhoon-botnet/727886.

25. Jaikaran, "Salt Typhoon Hacks."
26. Gyana Swain, "Salt Typhoon hacked the US National Guard for 9 months, and accessed networks in every state," *CSO*, July 16, 2025, https://www.csoonline.com/article/4023313/salt-typhoon-hacked-the-us-national-guard-for-9-months-and-accessed-networks-in-every-state.html.
27. David Jones, "What we know about the Microsoft SharePoint attacks," *Cybersecurity Dive*, July 24, 2025, https://www.cybersecuritydive.com/news/what-we-know-microsoft-sharepoint-attacks/753961.
28. David Dimolfetta, "Threat intel firms on alert for government systems impacted by Microsoft SharePoint vulnerability," *Nextgov FCW*, July 21, 2025, https://www.nextgov.com/cybersecurity/2025/07/threat-intel-firms-alert-government-systems-impacted-microsoft-sharepoint-vulnerability/406857.
29. Ibid.
30. "China Threat Overview and Advisories," CISA, September 17, 2025, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china.
31. "Joint ODNI, FBI, and CISA Statement," Federal Bureau of Investigation National Press Office, November 4, 2024, https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-110424.
32. Lambert, "Microsoft shifts."
33. "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," Government Accountability Office, April 22, 2021, accessed October 2025, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
34. "Supply Chain Compromise," CISA, January 7, 2021, https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise.
35. Anna Ribeiro, "Hackers target Tipton Municipal Utilities wastewater treatment plant, prompting federal investigation," *Industrial Cyber*, April 23, 2024, https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-tipton-municipal-utilities-wastewater-treatment-plant-prompting-federal-investigation; Sean Lyngaas, "Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says," *CNN Politics*, April 17, 2024, https://www.cnn.com/2024/04/17/politics/russia-hacking-group-suspected-texas-water-cyberattack/index.html.
36. Lambert, "Microsoft shifts."
37. "The Asymmetric Battlefield: An Anthropological and Geopolitical Analysis of Iranian Cyber Threats to North American Critical Infrastructure," Mjolnir Security, July 24, 2025, https://mjolnirsecurity.com/the-asymmetric-battlefield-an-anthropological-and-geopolitical-analysis-of-iranian-cyber-threats-to-north-american-critical-infrastructure.
38. Ibid.
39. Stephen Deere, "Feds: Iranians led cyberattack against Atlanta, other U.S. entities," *AJC Politics*, November 28, 2018, https://www.ajc.com/news/local-govt--politics/feds-iranians-led-cyberattack-against-atlanta-other-entities/xrLAyAwDroBvVGhp9bODyO.
40. Donnie O'Sullivan et al., Iranian hackers who posed as the Proud Boys accessed voter data in one state, feds say," *CNN Politics*, October 31, 2020, https://www.cnn.com/2020/10/30/politics/iran-hackers-proud-boys.

41. Trevor Laurence Jockims, "America's drinking water is facing attack, with links back to China, Russia and Iran," *CNBC*, June 26, 2024, https://www.cnbc.com/2024/06/26/americas-drinking-water-under-attack-china-russia-and-iran.html.
42. Jen Fifeild, "Hackers who breached election website aimed at other targets too," *AZ Mirror*, July 23, 2025, https://azmirror.com/2025/07/23/hackers-who-breached-arizona-election-website-aimed-at-other-targets-too.
43. Joseph Amankway-Amoah et al., "COVID-19 and digitalization: The great acceleration," *Journal of Business Research*, November 2021, 601-611, https://www.sciencedirect.com/science/article/pii/S0148296321005725.
44. "Benefits and Challenges of Cloud Adoption in Public Sector," App Maisters, September 2, 2025, https://gov.appmaisters.com/cloud-adoption-public-sector-benefits-challenges; "Cloud Computing: Federal Agencies Face Four Challenges," Government Accountability Office, September 28, 2022, https://www.gao.gov/products/gao-22-106195.
45. Kara Arundel et al., "School ransomware attacks are on the rise. What can districts do?" *K-12 Dive*, October 28, 2024, https://www.k12dive.com/news/school-ransomware-attacks-cybersecurity-funding/730333.
46. "MOVEit transfer data breaches Deep Dive," ORX, January 2024, https://orx.org/resource/moveit-transfer-data-breaches.
47. "What is a zero-day exploit?" IBM, accessed October 2025, https://www.ibm.com/think/topics/zero-day.
48. Sk Tahsin Hossain et al., "Cybersecurity in local governments: A systematic review and framework of key challenges," *Urban Governance*, March 2025, 1-19, https://www.sciencedirect.com/science/article/pii/S2664328624000792.
49. Conor Crimmins, "The Hidden Costs of Legacy Systems—and Why Government IT Modernization Can't Wait," Spider Strategies, September 18, 2025, https://www.spiderstrategies.com/blog/government-it-modernization.
50. "What was the WannaCry ransomware attack?" CloudFlare, accessed September 2025, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware.
51. Hossain et al., "Cybersecurity in local governments."
52. Harrison Mantas, "Fort Worth plugs holes with its IT system after weekend data breach," *Star-Telegram*, June 26, 2023, https://www.star-telegram.com/news/local/fort-worth/article276761706.html.
53. *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, Government Accountability Office, June 13, 2024, https://www.gao.gov/assets/gao-24-107231.pdf.
54. Tim Starks, "Congressional appropriators move to extend information-sharing law, fund CISA," *CyberScoop*, January 2026, https://cyberscoop.com/congressional-appropriators-move-to-extend-information-sharing-law-fund-cisa.
55. Anna Ribeiro, "US House Subcommittee reviews State and Local Cybersecurity Grant Program, considers adjustments for impact," *Industrial Cyber*, April 2, 2025, https://industrialcyber.co/threats-attacks/us-house-subcommittee-reviews-state-and-local-cybersecurity-grant-program-considers-adjustments-for-impact.
56. Colin Wood, "Cyber grant uncertainty puts state programs in limbo, GAO report shows," *StateScoop*, April 29, 2025, https://statescoop.com/dhs-state-local-cyber-grant-gao-report-2025.

57. Phillip Harmon, "Cybersecurity challenges faced by local governments in 2025," *SmartCities Dive*, March 14, 2025, https://www.smartcitiesdive.com/news/archive-acc-cybersecurity-challenges-faced-by-local-governments-in-2025/754778.
58. John MacMillan, "Enhancing Collaboration Across State and Local Government to Improve Cybersecurity Outcomes for Everyone," Pennsylvania Office of Administration, December 2020, https://www.nascio.org/wp-content/uploads/2021/08/PA-Cybersecurity-NASCIO-2021-Enhancing-Cyber-Collaboration-Across-State-and-Local-Government-FINAL.pdf.
59. Colin Wood, "New state, local cyber grant rules prohibit spending on MS-ISAC," *StateScoop*, August 4, 2025, https://statescoop.com/state-local-cyber-grant-msisac-2025.
60. Ibid.
61. Ibid.
62. Sophia Fox-Sowell, "To expand cyber workforce, government must unfreeze hiring and target youth, experts told House committee," *StateScoop*, February 5, 2025, https://statescoop.com/cybersecurity-workforce-house-committee-homeland-security.
63. "Why Federal Agencies Can't Find Top Tech Talent," CCS Global Tech, August 2025, https://ccsglobaltech.com/why-federal-agencies-cant-find-tech-talent.
64. Srini Subramanian and Meredith Ward, "2024 Deloitte-NASCIO Cybersecurity Study," Deloitte, September 2024, https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/2024-deloitte-nascio-cybersecurity-study.
65. Aaron K. Tantleff et al., "Cybersecurity in the Age of Industry 4.0," Foley & Ladner LLP, September 12, 2024, https://www.foley.com/insights/publications/2024/09/cybersecurity-industry-4-part-1.
66. Dave Stenger, "4 Threats to Cybersecurity for State and Local Governments," Ramp Xchange, March 3, 2025, https://rampxchange.com/blog/4-threats-to-cybersecurity-for-state-and-local-governments.
67. Jessica Balen, "Ransomware as a Service Threat Grows Against Local Governments," *State Tech*, March 2025, https://statetechmagazine.com/article/2025/03/ransomware-as-a-service-raas-perfcon.
68. "State and Local Cybersecurity: Facing New Burdens Amid Rising Threats," KnowBe4, March 2025, https://www.knowbe4.com/hubfs/Municipalities_Cybersecurity_Report.pdf.
69. David Jones, "State CISOs up against a growing threat environment with minimal funding, report finds," *Cybersecurity Dive*, October 2, 2024, https://www.cybersecuritydive.com/news/state-cisos-threat-funding/728686.
70. "New Report Highlights Critical Infrastructure Threats and the Role of State and Local Government Organizations in National Security," CIS, February 27, 2025, https://www.cisecurity.org/about-us/media/press-release/new-report-highlights-critical-infrastructure-threats-and-the-role-of-state-and-local-government-organizations-in-national-security.
71. Gary Barlet, "Matching cyber programs and partnerships with the pace of modern threats," *SmartCities Dive*, June 30, 2025, https://www.americancityandcounty.com/government-technology/matching-cyber-programs-and-partnerships-with-the-pace-of-modern-threats.
72. Jos Wetzels et al. "Insecure by Design in the Backbone of Critical Infrastructure," *CPS-IoT Week '23: Proceedings of Cyber-Physical Systems and Internet of Things Week 2023*, May 9, 2023, https://dl.acm.org/doi/10.1145/3576914.3587485.
73. "Cyber Security for Local Governments: The Challenges," Secon, September 18, 2024, https://seconcyber.com/cyber-security-for-local-governments-the-challenges.
74. "Why Vendor Risk Management Is Essential for Compliance?" MetricStream, accessed October 2025, https://www.metricstream.com/insights/5-best-practices-VRM.htm.
75. Michael Parisi, "Five Key Pitfalls in State and Local (SLED) Cybersecurity Compliance," Steel Patriot Partners, September 16, 2025, https://resources.steelpatriotpartners.com/key-pitfalls-state-and-local-

sled-cybersecurity; Nick Kuriger, "Cybersecurity in Local Government: Navigating Compliance and Risk," EC-Council Cybersecurity Exchange, September 25, 2025, https://www.eccouncil.org/cybersecurity-exchange/executive-management/local-government-cybersecurity-compliance-risk.

76. "Software Acquisition Guide for Government Enterprise Consumers," Software Assurance Work Group, August 2024, https://www.cisa.gov/sites/default/files/2024-07/PDM24050%20Software%20Acquisition%20Guide%20for%20Government%20Enterprise%20ConsumersV2_508c.pdf.
77. Georgia Collins, "HP: Supply Chain Security Failures are Costing Billions," *SupplyChain Digital*, December 2024, https://supplychaindigital.com/technology/hp-procurement-supply-chain-security-failings.
78. Brandi Steckel et al., "Whole-of-state cybersecurity: Three procurement considerations for the public sector," Amazon, April 13, 2023, https://aws.amazon.com/blogs/publicsector/whole-state-cybersecurity-three-procurement-considerations-public-sector.
79. Anthony Cogswell, "6 cybersecurity challenges for state and local governments," *WatchGuard*, July 21, 2023, https://www.watchguard.com/wgrd-news/blog/6-cybersecurity-challenges-state-and-local-governments-0.
80. *High-Risk Series*, Government Accountability Office.
81. Emil Sayegh, "The DHS Funding Lapse Is A Cyber Resilience Test," *Forbes*, February 17, 2026, https://www.forbes.com/sites/emilsayegh/2026/02/17/the-dhs-funding-lapse-is-a-cyber-resilience-test.
82. Dave Stenger, "State and Local Governments' Cybersecurity Challenges," Ramp Xchange, March 3, 2025, https://rampxchange.com/blog/state-and-local-governments-cybersecurity-challenges.
83. Rae D. DeShong, "A Reauthorized SLCGP Still Doesn't Escape DHS Shutdown," Government Technology, February 17, 2026, https://www.govtech.com/security/a-reauthorized-slcgp-still-doesnt-escape-dhs-shutdown.
84. Rae D. DeShong, "Congress Moves to Revive State and Local Cybersecurity Grant Program," Government Technology, November 19, 2025, https://www.govtech.com/security/congress-moves-to-revive-state-and-local-cybersecurity-grant-program.
85. Mickey McCarter, "Congress Revives State and Local Cyber Grants, But Funding Remains Unclear," StateTech, November 24, 2025, https://statetechmagazine.com/article/2025/11/congress-revives-state-and-local-cyber-grants-funding-remains-unclear.
86. Gray Oshin, "How the CyberCorps is preparing tomorrow's workforce," *Cybersecurity Guide*, October 24, 2025, https://cybersecurityguide.org/resources/cybercorps/.
87. NSF 21-580: CyberCorps(R) Scholarship for Service (SFS), U.S. National Science Foundation, April 23, 2021, https://www.nsf.gov/funding/opportunities/cyberai-sfs-cyberaicorps-scholarship-service/504991/nsf21-580/solicitation.
88. David Kertai, "Texas's New Cyber Command Offers a Model for Other States" (ITIF, June 16, 2025), https://itif.org/publications/2025/06/16/texas-new-cyber-command-offers-a-model-for-other-states.
89. Sophia Fox-Sowell, "Texas governor signs bill for statewide Cyber Command," *StateScoop*, June 4, 2025, https://statescoop.com/texas-cyber-command-gov-abbott.
90. Jeff Greene et al., "The Limits of Risk-Informed Planning for State and Local Cyber Readiness," Aspen Digital, June 5, 2025, https://www.aspendigital.org/blog/state-and-local-cyber-readiness.
91. Stenger, "State and Local Governments' Cybersecurity Challenges."
92. "CISA Regions," CISA, accessed September 2025, https://www.cisa.gov/about/regions.

93. U.S. Department of Justice Office of the Inspector General, "DOJ OIG Releases Report on DOJ's Strategy to Combat and Respond to Ransomware Threats and Attacks," United States Government, September 17, 2024, https://oig.justice.gov/news/doj-oig-releases-report-dojs-strategy-combat-and-respond-ransomware-threats-and-attacks; U.S. Government Accountability Office, "Ransomware: Federal Coordination and Assistance Challenges," United States Government, November 16, 2022, https://www.gao.gov/products/gao-23-106279.
94. Jaikumar Vijayan, "What is an ISAC or ISAO? How these cyber threat information sharing organizations improve security," *CSO*, July 26, 2022, https://www.csoonline.com/article/567485/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.
95. Kertai, "Texas's New Cyber."
96. Emergency Management Assistance Compact (EMAC), "The EMAC Process," EMAC, 2026, https://www.emacweb.org/index.php/how-emac-works; Cybersecurity and Infrastructure Security Agency, "Emergency Management Assistance Compact Package," CISA, 2017, https://www.cisa.gov/sites/default/files/publications/EMAC%20Package_FINAL_508.pdf.
97. Fox-Sowell, "Texas governor signs bill."
98. Colin Wood, "Per new law, all New York agencies required to take cyber awareness training," *StateScoop*, June 30, 2025, https://statescoop.com/new-york-cybersecurity-training-awareness-hochul.
99. Daniel Castro, "Hit with a Ransomware Attack? Don't Pay the Hackers," Government Technology, September 2019, https://www.govtech.com/opinion/hit-with-a-ransomware-attack-dont-pay-the-hackers.html.
100. Karen Painter Randall, "Two States Now Prohibit Public Entities from Paying Ransoms," Connell Foley LLP, August 18, 2022, https://www.connellfoley.com/blog/Two-States-Prohibit-Public-Entities-Paying-Ransoms.
101. "Governor Hochul Signs Landmark Legislation to Strengthen Cybersecurity Across New York's Municipalities," New York State Governor's Office, June 27, 2025, https://www.governor.ny.gov/news/governor-hochul-signs-landmark-legislation-strengthen-cybersecurity-across-new-yorks.
102. Ibid.
103. Tim Callan, "How Can State and Local Government Institutions Strengthen Cybersecurity in 2026," Sectigo, January 6, 2026, https://www.sectigo.com/blog/state-local-government-cybersecurity-strategies.
104. "CISA Unveils Tool to Boost Procurement of Software Supply Chain Security," CISA, August 26, 2025, https://www.cisa.gov/news-events/news/cisa-unveils-tool-boost-procurement-software-supply-chain-security.
105. "Governor Hochul Signs," New York State Governor's Office.
106. Baily, Jr., "Federal agency investigating"; Rodas, "Ransomware attack causes."
107. "Nation-State Threats," CISA.