Division of Local Government
and School Accountability

Cyber Profile

October 2023

Thomas P. DiNapoli OFFICE OF THE NEW YORK STATE COMPTROLLER

New York Local Government and School Cybersecurity: A Cyber Profile

Cybersecurity is a national security imperative.[1] Local governments and schools across the United States, including those in New York, are at risk of cyberattack. In recent years local governments and schools have been a common target.[2]

Cybersecurity underpins most local government and school operations, and its resiliency is essential for safeguarding networks, devices and data from unauthorized access or criminal use while ensuring confidentiality, integrity and availability of information.[3] The importance of a strong cybersecurity posture cannot be overstated.

This publication profiles:

- Cybersecurity challenges facing New York's local governments and schools.
- Perspectives and insights from local and school officials on key cybersecurity topics.
- The Office of the State Comptroller's local government and school cybersecurity action plan:
  - Audits, common findings and recommendations
  - On demand resources for local government and school officials
- Other resources.

Cybersecurity is a national security imperative.

Contents

Cybersecurity Challenges Facing New York State's Local Governments and Schools

In New York, cyberattacks have impacted local governments and schools both large and small, including reported attacks at counties including Albany, Chenango, Erie, Nassau, Schenectady and Schuyler; cities including New York, Buffalo, Yonkers, Long Beach and Olean; towns including Brookhaven, Ulster, Canandaigua and Moreau; and schools including Buffalo Public Schools and the Guilderland Central School District.[4] Suffolk County is still dealing with the impact of a ransomware attack.

These and other recent events have demonstrated the potential for unauthorized access to personal, private and sensitive information and significant impact to critical local government and school operations that have become heavily reliant on technology. The risk is severe.[5]

Yet, resources and responsibility designation for helping protect such information and operations has not consistently kept pace. New York's local government and school information technology (IT) and cybersecurity efforts could be led by their own IT department staff, by staff who, in addition to IT, have other responsibilities (e.g., Business office or other operational duties) or could be led by contracted third-party IT and cybersecurity personnel.

Cyberattacks pose a fiscal risk and can impact public safety and well-being when targeting local government operations including those managing emergency communications, water systems, other utilities, airports, healthcare facilities and schools.[6]

Certain cyberattacks come in the form of ransomware, disrupting access to technology and, in some instances, threatening to disclose confidential or otherwise sensitive data to the public unless a ransom payment is made. Ransomware can severely impact operations and leave local government and school officials without the data they need to deliver mission-critical services upon which the public depends. Local governments and schools of all sizes have been challenged by the economic and reputational impacts of ransomware, from the initial disruption through the often-extended recovery.[7]

Incorporating smart technology has also opened the door to significant new risks at local governments and schools. Such technology generates and collects massive amounts of data about local government and school operations, residents and students. As public stewards, local government and school officials face heightened challenges and responsibilities to ensure privacy and security while simultaneously storing, analyzing, sharing and applying this data for capability enhancements.

The United States Government Accountability Office (GAO) first designated information security as a government-wide high-risk area in 1997. In 2003, this high-risk area was expanded to include the protection of critical cyber infrastructure and, in 2015, the privacy of personally identifiable information.[8]

In November 2022, the GAO warned the United States Department of Education that its plan for addressing risks in schools needed to be updated to include current cyber threats, and that schools could benefit from more specific cybersecurity guidance. Such threats and guidance are increasingly important given the additional burden placed on schools when their networks grant access to large numbers of devices, some of which students and others use outside of school for remote learning.[9]

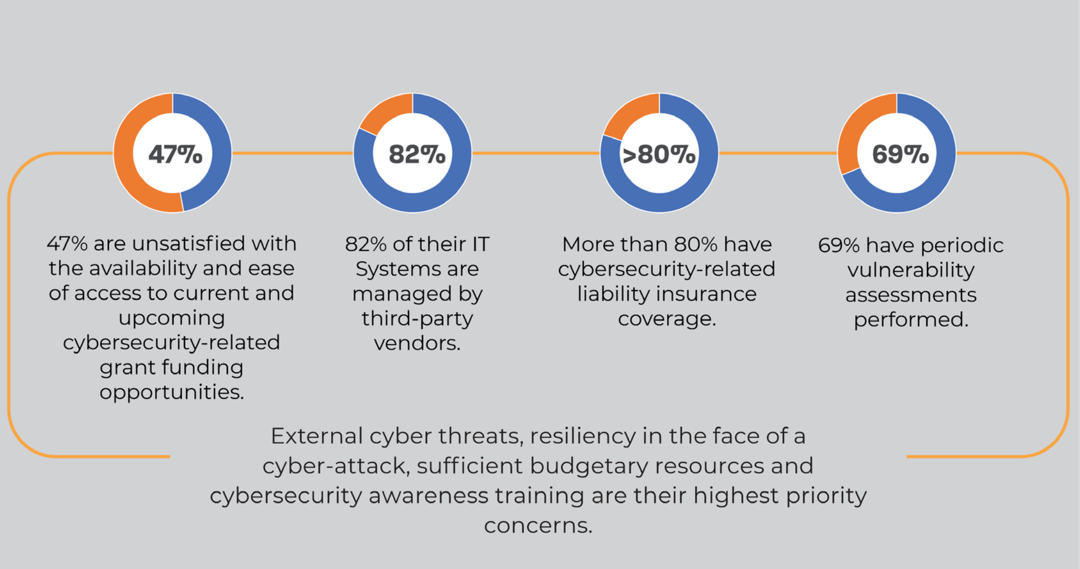
Cybersecurity has taken on a renewed sense of urgency across the United States. Constant cyberattacks originating from foreign countries or on behalf of foreign governments, along with increasingly sophisticated perpetrators, make efforts to stay a step ahead imperative. Tackling the problem takes more than expertise and tools to monitor and protect against attacks. As local governments and schools continue to be targets, knowing how to prepare for and respond to cyberattacks is essential.[10] To this end, the recommended cyber defensive posture includes both prevention as well as one of resilience and recovery.[11]

New York State’s Local Government and School Officials’ Perspectives on Cybersecurity Challenges

In November 2022, the Office of the State Comptroller’s Division of Local Government and School Accountability (LGSA) distributed a survey to approximately 2,300 local government and school officials to hear their perspectives regarding the cybersecurity challenges they face in their counties, cities, towns, villages and schools. The survey inquired about local government and school cybersecurity profiles, practices, priorities and concerns, and focused on topics such as:

- Operational profile highlights.
- Cybersecurity hygiene, a set of practices performed regularly to help maintain the cyber health and security of networks, devices, data and users.
- Local government and school cybersecurity threats.
- Cybersecurity funding resources.

Over 900 officials, or nearly 40 percent of recipients, responded to the survey. While the responses included certain sensitive or confidential information, when aggregated, they identified some high-level and commonly occurring themes among the survey respondents. For example, in addition to providing information about critical infrastructure and whether contracts and/or service level agreements are established with third-party Information Technology (IT) support providers, the survey responses provided other valuable insight, as shown in the graphic below.



47% are unsatisfied with the availability and ease of access to current and upcoming cybersecurity-related grant funding opportunities.

82% of their IT Systems are managed by third-party vendors.

More than 80% have cybersecurity-related liability insurance coverage.

69% have periodic vulnerability assessments performed.

External cyber threats, resiliency in the face of a cyber-attack, sufficient budgetary resources and cybersecurity awareness training are their highest priority concerns.

LGSA’s Cybersecurity Action Plan

The Division of Local Government and School Accountability oversight of local governments and schools is accomplished, in part, through risk assessments and audits. LGSA also provides training and technical assistance, issues guidance through publications and research reports, and facilitates reporting requirements and proposing legislation. This work helps OSC ensure public accountability and improve governance, performance and operations at all levels.

LGSA’s Cybersecurity Audits

The Office of the State Comptroller’s LGSA audits identify fundamental weaknesses in local government and school cyber defenses to help these entities improve their efforts to prevent cyberattacks.

From January 1, 2019 through July 31, 2023, LGSA released more than 190 IT-related audits, reporting on nearly 2,400 IT findings. The IT-related audit findings to date center on breakdowns or gaps in fundamental and foundational cybersecurity components. Drawing from our audit findings, the most common categories where improvement and corrective action recommendations were needed include:

> The Office of the State Comptroller’s LGSA audits identify fundamental weaknesses in local government and school cyber defenses to help these entities improve their efforts to prevent cyberattacks.

- **Policies and Procedures —** Cyber hygiene and personal, private and sensitive information protection guidance and protocols should be established and distributed to all IT users, and compliance should be monitored and enforced.
- **IT Security Awareness Training —** A well-informed workforce is essential to securing electronic data and IT systems. This training should explain the proper rules of behavior for using IT systems and data and communicate the policies and procedures that need to be followed.
- **IT Contingency Plan —** Proactively anticipating and planning for cyber disruptions prepares personnel for the needed actions in the event of an actual disruption and could significantly reduce the resulting impact.
- **Internet Use —** Websites should be accessed only for appropriate purposes and from trusted sources.

- **Access Controls —** User account access and permissions should be granted only to authorized IT users and for appropriate purposes. The passwords used to access those accounts should be sufficiently long, unique or complex, and reset immediately upon evidence of a compromise or periodically otherwise.
- **Computer and Network Security —** Cybersecurity is an ongoing process requiring constant attention to regular software updates, malware protection, actively managed remote access and controlled mobile device use.

LGSA's audits regularly identify cybersecurity-related findings which are sensitive in nature. Those findings and recommendations for corrective action are communicated confidentially to local government and school officials.

Our audit and assessment efforts offer targeted recommendations for corrective action, many of which can be implemented at no or low cost to the local government or school being audited.

Our audit and assessment efforts offer targeted recommendations for corrective action, many of which can be implemented at no or low cost to the local government or school being audited.

LGSA's Cybersecurity Resources Available to Local Government and School Officials

Cybersecurity threats are an ever-present organizational risk on par with economic, legal, operational, financial and political risks. Managing these risks, and the threats from which they stem, is one part of an overall risk management program. A successful risk management program requires effective governance, encompassing the processes by which risk decisions are made.[12]

Local government and school officials should treat cybersecurity risks as they do any other hazard they encounter: identify the risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the governing board, the chief executive officer, and others responsible to help manage and secure a local government's or school's IT assets.[13]

Although no single practice or policy on its own can adequately safeguard these assets from cybersecurity risks, there are several IT governance efforts that, if properly enacted and monitored, collectively increase the odds IT assets will remain safe. In addition to LGSA's audit findings and recommendations, LGSA provides several other resources to help assist board members and local government and school officials in such IT governance efforts.

One highlight is LGSA's *Information Technology Governance Local Government Management Guide* (LGMG), containing a cybersecurity self-assessment tool designed to help boards and officials assess the local government's or school's IT environment and recovery readiness. This comprehensive tool is structured around 12 key areas of cybersecurity and is intended to help boards and officials exercise effective cybersecurity oversight.

Additional LGSA cybersecurity-related resources for local and school officials include:

- Cybersecurity Local Government Management Guides (LGMGs) —

  LGSA offers a series of publications, LGMGs, that provide guidance on several management and technical topics. The following LGMGs focus on key topics within IT and cybersecurity:

  - Ransomware
  - Information Technology Contingency Planning
  - Wireless Technology and Security
  - Industrial Control Systems Cybersecurity

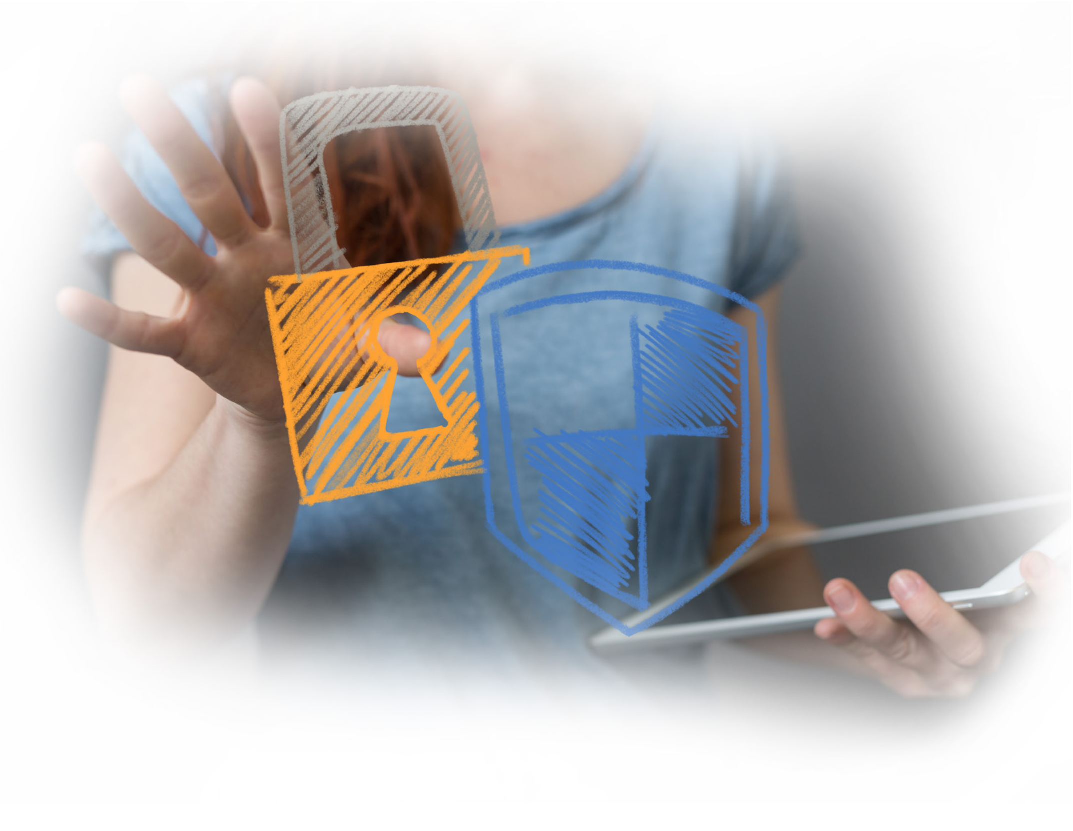
- Cybersecurity Training Webinars —

  LGSA offers webinars for local government and school officials covering a wide range of training topics on demand and available for officials at their convenience. Annually, LGSA recognizes October as National Cybersecurity Awareness Month by releasing weekly webinars highlighting key cybersecurity topics such as Cybersecurity Foundations and IT Governance, Ransomware and Multifactor Authentication.

The Academy

Sponsored by the Division of Local Government and School Accountability

Office of the New York State Comptroller
THOMAS P. DiNAPOLI



  - 2023
    - Week 1 — Proactive Cybersecurity Steps for Local Governments and Schools — Part 1
    - Week 2 — Cybersecurity Governance for Local Governments and Schools — Part 2
  - 2022
    - Week 1 — Cybersecurity Foundations
    - Week 2 — Software Management
    - Week 3 — Multifactor Authentication
    - Week 4 — Passwords
    - Week 5 — Phishing
  - 2021
    - Week 1 — IT Governance
    - Week 2 — IT Contingency Planning
    - Week 3 — Wireless Security and Technology
    - Week 4 — Ransomware
  - 2020
    - Week 1 — Where Do We Start?
    - Week 2 — We Are Our Own Biggest Threat
    - Week 3 — Protecting Against Unseen Dangers
    - Week 4 — Tying Up Loose Ends

- Cybersecurity Research Reports and Other Publications —

  LGSA releases reports and other publications on major policy issues facing local governments, schools and State policymakers. Publications focused on IT and cybersecurity include:

  - Smart Solutions Across the State: Advanced Technology in Local Governments
  - Local Government Information Security: The Cost of Inadequate Protections
  - Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders

Office of the NEW YORK STATE COMPTROLLER

Smart Solutions Across the State: Advanced Technology in Local Governments

Local Government Snapshot

NEW YORK STATE OFFICE OF THE STATE COMPTROLLER

Thomas P. DiNapoli • State Comptroller

August 2011

Local Government Information Security: The Cost of Inadequate Protections

Office of the NEW YORK STATE COMPTROLLER

Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders

Other Cybersecurity Resources Available to Local Government and School Officials

New York State takes a "Whole-of-State" approach to cybersecurity, emphasizing partnerships, particularly among State agencies and localities, to collectively enhance cybersecurity across communities throughout the State.[14] Advancing this priority, in August 2023, Governor Kathy Hochul announced the release of New York's Cybersecurity Strategy which sets forth "a nation-leading blueprint to ensure New York State stands ready and resilient in the face of cyber threats."[15] Additionally, some of New York State's cybersecurity efforts include:

- The Division of Homeland Security and Emergency Services' Cyber Incident Response Team, established in 2017 to provide cyber incident response and other cybersecurity services such as risk assessments and training.[16] These services are available at no cost to local governments.
- The creation of a Joint Security Operations Center in February 2022 to serve as the nerve center for joint local, State and federal cyber efforts, including data collection, response and information sharing.[17]
- A $30 million shared services program announced in July 2022 to assist counties with cybersecurity, including thorough tools to help protect against ransomware attacks.[18]

Similarly, New York State's Education Department promotes policies and practices at schools and other State educational agencies that help strengthen data privacy and security.[19] The Education Department issued regulations in 2020 for protecting student data and annual professional performance review data,[20] provide resources for educational agencies' data protection officers[21] and collects reports of data privacy and security incidents from schools and other educational agencies.[22]

Associations that offer cybersecurity resources to local and school officials include:

- New York State Association of Counties

  Publications:

  - Cybersecurity Primer for Local Government Leaders
  - Cybersecurity Insurance Challenges for Public Entities
  - Cybersecurity Tabletop Exercises for Local Governments

- New York State Conference of Mayors

  Publications:

  - A Proactive Approach to Cyber Security
  - Don’t Be Held Ransom: Being Cyber Aware — Protecting Your Municipality
  - Is Your Municipal Water Safe From a Cyber Attack?

- New York State School Boards Association

  Online Learning:

  - Social Media and You

- New York State RIC One

  Twelve Regional Information Centers (RICs) working as one to provide statewide technology leadership and innovative solutions.

  Publications:

  - Data Protection and Planning Guide
  - NIST Framework District Readiness Tool

  Podcast:

  - DPO (Data Protection Officer) Download Podcast

In addition, Office of the State Comptroller auditors and IT specialists regularly participate in panel discussions and lead in-person workshops at cybersecurity and audit-related events across the State, including those sponsored by various local government and school associations. LGSA's ongoing cybersecurity-related work, including audits and technical assistance, publications and training, and partnerships, complement these and other Whole-of-State efforts to support strengthening local government and school proactive cybersecurity assessment, recovery and resilience.

Endnotes

1 White House, “Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity,” August 25, 2021 at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

2 Government Technology, “The Increasing Concern of Public-Sector Cybersecurity in State and Local Government,” September 29, 2022 at https://www.govtech.com/sponsored/the-increasing-concern-of-public-sector-cybersecurity-in-state-and-local-government.

3 United States Cybersecurity and Infrastructure Security Agency, “What is Cybersecurity?,” February 1, 2021 at https://www.cisa.gov/news-events/news/what-cybersecurity.

4 Office of the New York State Comptroller, press release (New York Needs to Improve Cybersecurity Support), November 12, 2021 at https://www.osc.state.ny.us/press/releases/2021/11/dinapoli-new-york-needs-improve-cybersecurity-support-local-governments-and-public-authorities.

5 United States Cybersecurity and Infrastructure Security Agency, Partnering to Safeguard Localities from Cybersecurity Threats Toolkit (accessed June 20, 2023).

6 United States Cybersecurity and Infrastructure Security Agency, Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats, January 19, 2023.

7 United States Cybersecurity and Infrastructure Security Agency, “Stop Ransomware,” at https://www.cisa.gov/stopransomware (accessed June 20, 2023).

8 United States Government Accountability Office, “Cybersecurity,” at https://www.gao.gov/cybersecurity (accessed June 20, 2023).

9 United States Government Accountability Office, Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity, October 2022.

10 National Conference of State Legislatures, “With Attacks on the Rise, Lawmakers Harden Cybersecurity,” March 15, 2022 at https://www.ncsl.org/state-legislatures-news/details/with-attacks-on-the-rise-lawmakers-harden-cybersecurity.

11 Government Technology, “3 Steps to Help State and Local Governments Build Cyber Resilience,” November 4, 2022 at https://www.govtech.com/sponsored/3-steps-to-help-state-and-local-governments-build-cyber-resilience.

12 University at Albany’s Center for Technology in Government, *Managing Cyber Threats through Effective Governance: A Call to Action for Governors and State Legislatures*, October 2020 at https://www.ctg.albany.edu/media/pubs/pdfs/managing_cyber_threats_through_effective_governance.pdf.

13 United States Cybersecurity and Infrastructure Security Agency, Cyber Essentials Element: Yourself, The Leader, May 29, 2020.

14 Governor Kathy Hochul, press release (Expansion of State’s Major Investments in Cybersecurity Initiatives), January 10, 2023 at https://www.governor.ny.gov/news/governor-hochul-announces-expansion-states-major-investments-cybersecurity-initiatives.

15 Governor Kathy Hochul, press release (Announcement of Nation-Leading Cybersecurity Strategy), August 9, 2023 at https://www.governor.ny.gov/news/governor-hochul-announces-nation-leading-cybersecurity-strategy.

16 New York Division of Homeland Security and Emergency Services, “Cyber Incident Response Team,” at https://www.dhses.ny.gov/cyber-incident-response-team (accessed June 20, 2023).

17 Governor Kathy Hochul, press release (Formation of Joint Security Operations Center to Oversee Cybersecurity Across the State), February 22, 2022 at https://www.governor.ny.gov/news/governor-hochul-announces-formation-joint-security-operations-center-oversee-cybersecurity.

18 Governor Kathy Hochul press release (Launch of $30 Million Shared Services Program to Enhance Cyber Defenses in Counties Across the State), July 21, 2022 at https://www.governor.ny.gov/news/governor-hochul-announces-launch-30-million-shared-services-program-enhance-cyber-defenses.

19 New York State Education Department, “Data Privacy and Security,” at https://www.nysed.gov/data-privacy-security (accessed June 20, 2023).

20 New York State Education Department, “Part 121 of the Regulations of the Commissioner of Education,” at https://www.nysed.gov/data-privacy-security/regulations-strengthen-data-privacy-and-security (accessed June 20, 2023).

21 New York State Education Department, “Data Protection Officer Resources,” at https://www.nysed.gov/data-privacy-security/data-protection-officer-resources (accessed June 20, 2023).

22 New York State Education Department, “Agencies: Report a Data Privacy/Security Incident,” at https://www.nysed.gov/data-privacy-security/agencies-report-data-privacysecurity-incident (accessed June 20, 2023).

Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.state.ny.us

Prepared by LGSA Applied Technology Unit