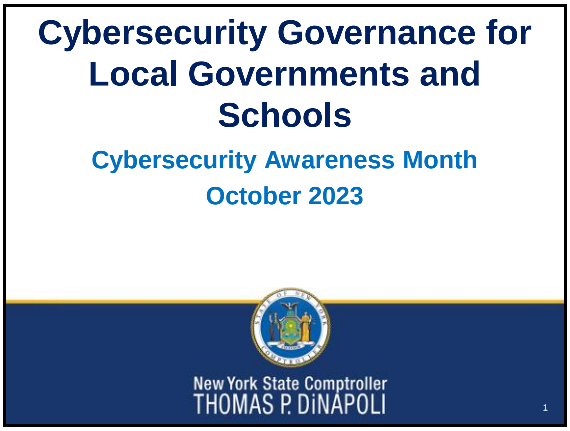


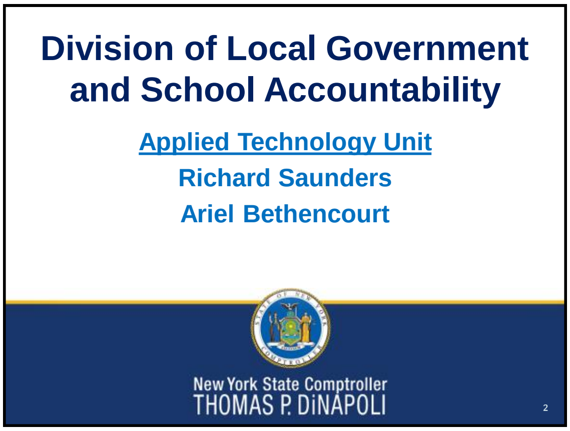
Cybersecurity Governance for Local Governments and Schools

Cybersecurity Awareness Month

October 2023

New York State Comptroller
THOMAS P. DiNAPOLI

1



Division of Local Government and School Accountability

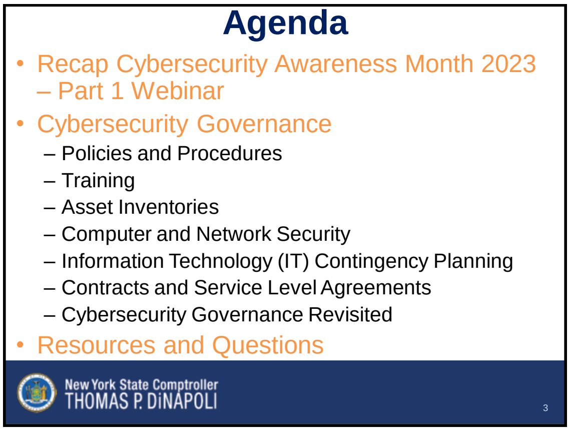
Applied Technology Unit

Richard Saunders

Ariel Bethencourt

New York State Comptroller
THOMAS P. DiNAPOLI

2

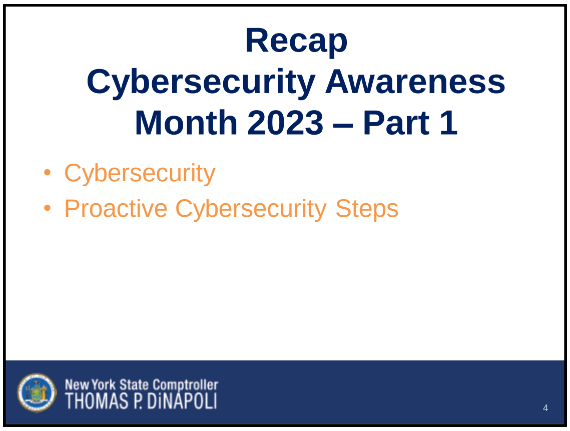


Agenda

- Recap Cybersecurity Awareness Month 2023 – Part 1 Webinar
- Cybersecurity Governance
  - Policies and Procedures
  - Training
  - Asset Inventories
  - Computer and Network Security
  - Information Technology (IT) Contingency Planning
  - Contracts and Service Level Agreements
  - Cybersecurity Governance Revisited
- Resources and Questions

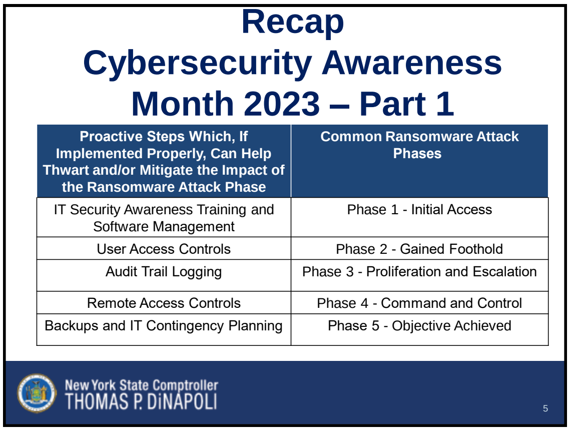
New York State Comptroller
THOMAS P. DiNAPOLI

3



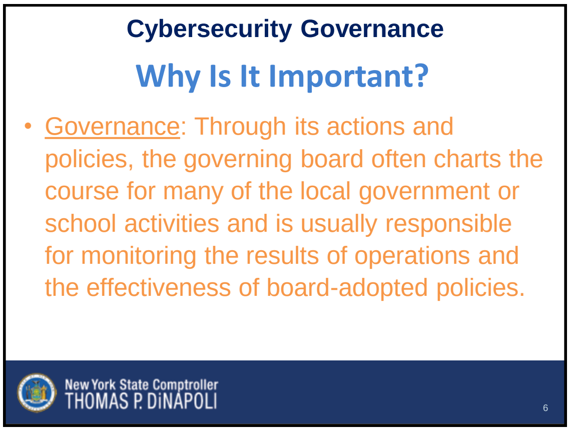
Recap Cybersecurity Awareness Month 2023 – Part 1

- Cybersecurity
- Proactive Cybersecurity Steps



Recap Cybersecurity Awareness Month 2023 – Part 1

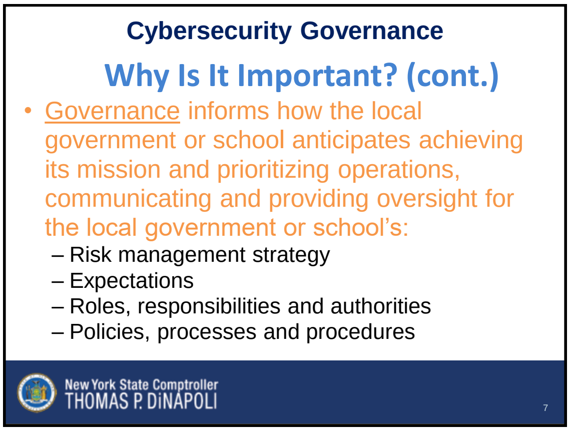
Proactive Steps Which, If Implemented Properly, Can Help Thwart and/or Mitigate the Impact of the Ransomware Attack Phase	Common Ransomware Attack Phases
IT Security Awareness Training and Software Management	Phase 1 - Initial Access
User Access Controls	Phase 2 - Gained Foothold
Audit Trail Logging	Phase 3 - Proliferation and Escalation
Remote Access Controls	Phase 4 - Command and Control
Backups and IT Contingency Planning	Phase 5 - Objective Achieved



Cybersecurity Governance

Why Is It Important?

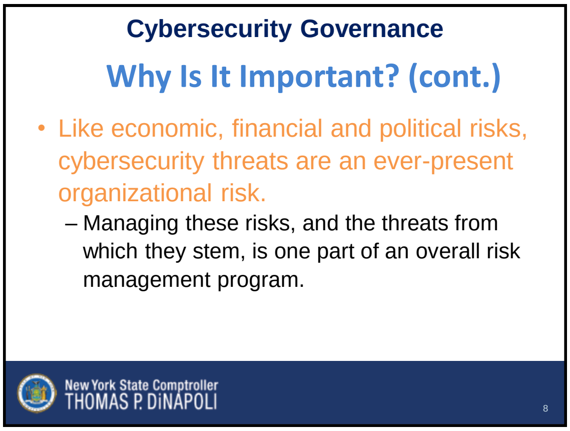
- Governance: Through its actions and policies, the governing board often charts the course for many of the local government or school activities and is usually responsible for monitoring the results of operations and the effectiveness of board-adopted policies.



Cybersecurity Governance

Why Is It Important? (cont.)

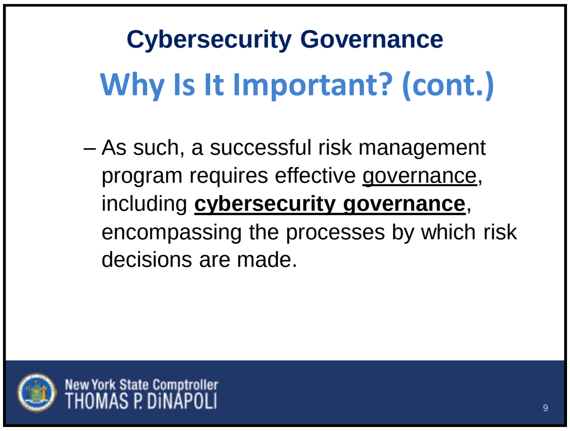
- Governance informs how the local government or school anticipates achieving its mission and prioritizing operations, communicating and providing oversight for the local government or school's:
  - Risk management strategy
  - Expectations
  - Roles, responsibilities and authorities
  - Policies, processes and procedures



Cybersecurity Governance

Why Is It Important? (cont.)

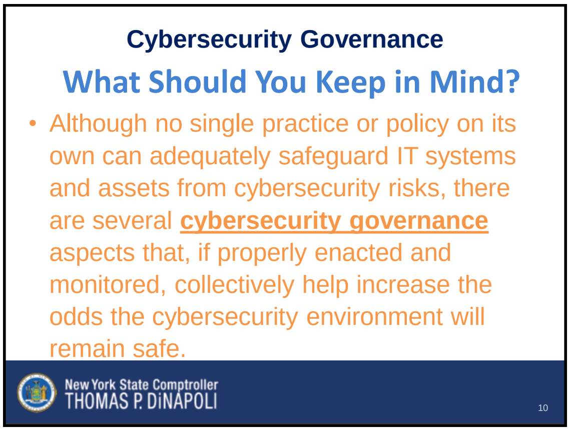
- Like economic, financial and political risks, cybersecurity threats are an ever-present organizational risk.
  - Managing these risks, and the threats from which they stem, is one part of an overall risk management program.



Cybersecurity Governance

Why Is It Important? (cont.)

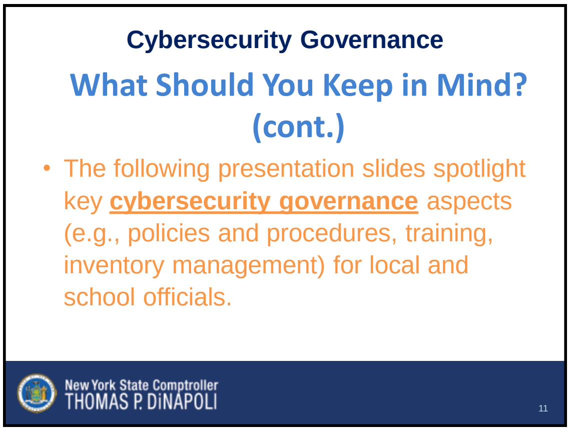
- As such, a successful risk management program requires effective governance, including **cybersecurity governance**, encompassing the processes by which risk decisions are made.



Cybersecurity Governance

What Should You Keep in Mind?

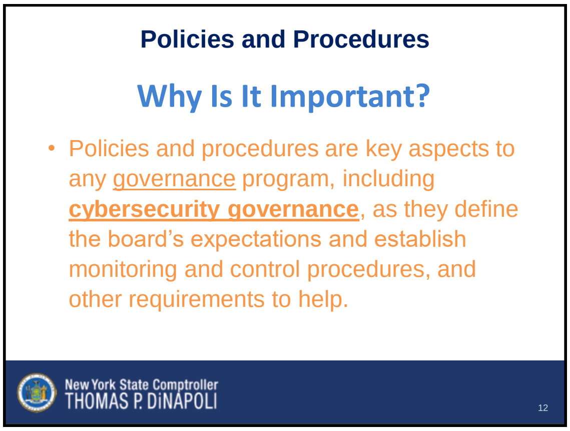
- Although no single practice or policy on its own can adequately safeguard IT systems and assets from cybersecurity risks, there are several **cybersecurity governance** aspects that, if properly enacted and monitored, collectively help increase the odds the cybersecurity environment will remain safe.



Cybersecurity Governance

What Should You Keep in Mind? (cont.)

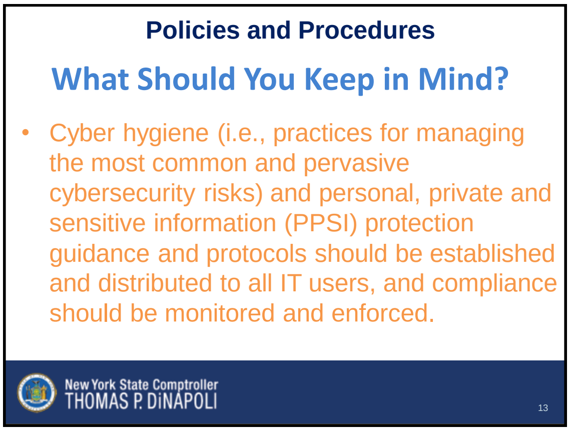
- The following presentation slides spotlight key **cybersecurity governance** aspects (e.g., policies and procedures, training, inventory management) for local and school officials.



Policies and Procedures

Why Is It Important?

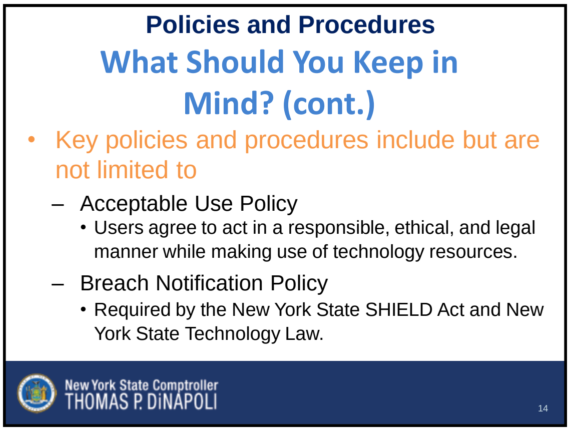
- Policies and procedures are key aspects to any governance program, including **cybersecurity governance**, as they define the board’s expectations and establish monitoring and control procedures, and other requirements to help.



Policies and Procedures

What Should You Keep in Mind?

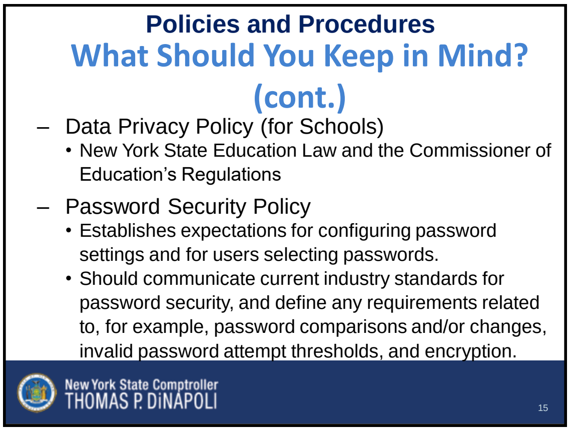
- Cyber hygiene (i.e., practices for managing the most common and pervasive cybersecurity risks) and personal, private and sensitive information (PPSI) protection guidance and protocols should be established and distributed to all IT users, and compliance should be monitored and enforced.



Policies and Procedures

What Should You Keep in Mind? (cont.)

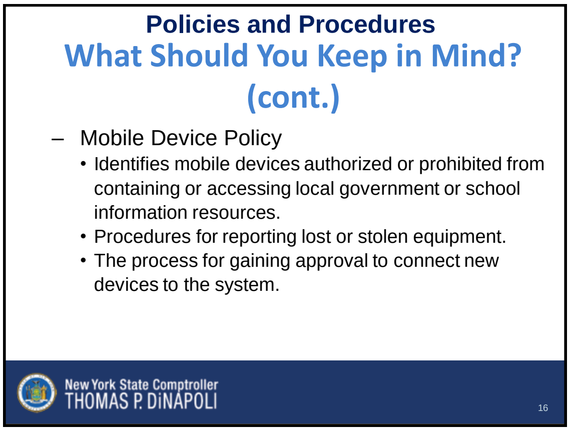
- Key policies and procedures include but are not limited to
  - Acceptable Use Policy
    - Users agree to act in a responsible, ethical, and legal manner while making use of technology resources.
  - Breach Notification Policy
    - Required by the New York State SHIELD Act and New York State Technology Law.



Policies and Procedures

What Should You Keep in Mind? (cont.)

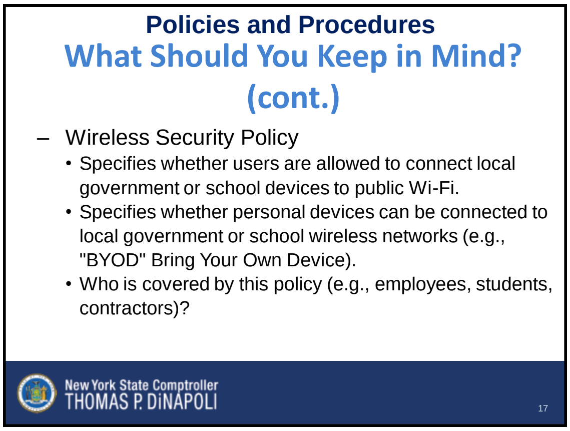
- Data Privacy Policy (for Schools)
  - New York State Education Law and the Commissioner of Education’s Regulations
- Password Security Policy
  - Establishes expectations for configuring password settings and for users selecting passwords.
  - Should communicate current industry standards for password security, and define any requirements related to, for example, password comparisons and/or changes, invalid password attempt thresholds, and encryption.



Policies and Procedures
What Should You Keep in Mind? (cont.)

- Mobile Device Policy
  - Identifies mobile devices authorized or prohibited from containing or accessing local government or school information resources.
  - Procedures for reporting lost or stolen equipment.
  - The process for gaining approval to connect new devices to the system.

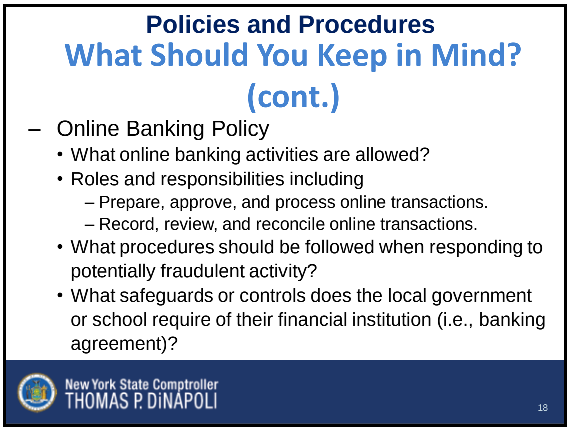
New York State Comptroller
THOMAS P. DiNAPOLI



Policies and Procedures
What Should You Keep in Mind? (cont.)

- Wireless Security Policy
  - Specifies whether users are allowed to connect local government or school devices to public Wi-Fi.
  - Specifies whether personal devices can be connected to local government or school wireless networks (e.g., "BYOD" Bring Your Own Device).
  - Who is covered by this policy (e.g., employees, students, contractors)?

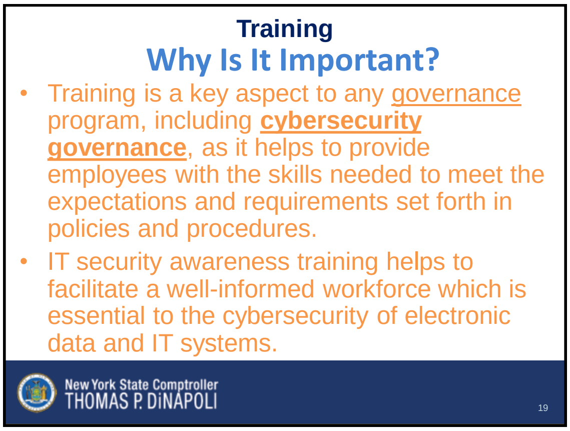
New York State Comptroller
THOMAS P. DiNAPOLI



Policies and Procedures
What Should You Keep in Mind? (cont.)

- Online Banking Policy
  - What online banking activities are allowed?
  - Roles and responsibilities including
    - Prepare, approve, and process online transactions.
    - Record, review, and reconcile online transactions.
  - What procedures should be followed when responding to potentially fraudulent activity?
  - What safeguards or controls does the local government or school require of their financial institution (i.e., banking agreement)?

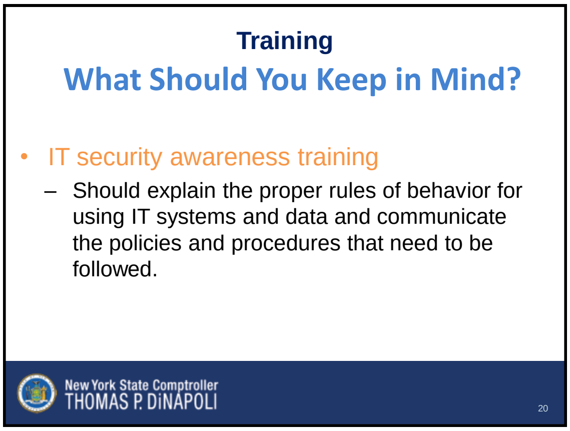
New York State Comptroller
THOMAS P. DiNAPOLI



Training

Why Is It Important?

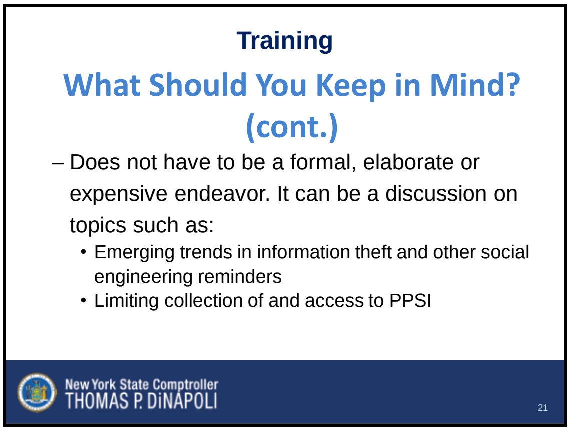
- Training is a key aspect to any governance program, including **cybersecurity governance**, as it helps to provide employees with the skills needed to meet the expectations and requirements set forth in policies and procedures.
- IT security awareness training helps to facilitate a well-informed workforce which is essential to the cybersecurity of electronic data and IT systems.



Training

What Should You Keep in Mind?

- IT security awareness 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.



Training

What Should You Keep in Mind? (cont.)

– Does not have to be a formal, elaborate or expensive endeavor. It can be a discussion on topics such as:
  - Emerging trends in information theft and other social engineering reminders
  - Limiting collection of and access to PPSI

Training

What Should You Keep in Mind? (cont.)

- The dangers of downloading files and programs from the Internet.
- How to respond if a malware or information breach is detected.
- Key IT security controls such as strong passwords, malware protection or wireless security.

Asset Inventories

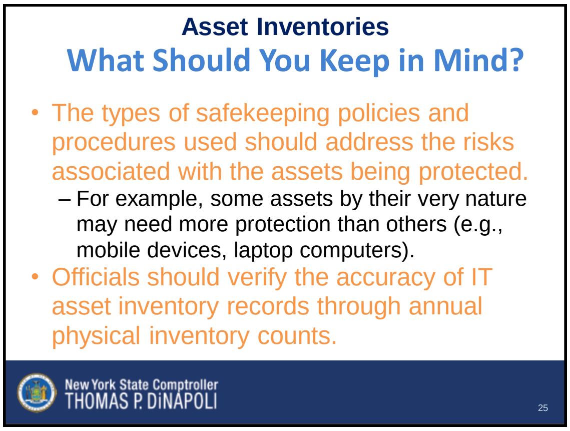
Why Is It Important?

- Local governments and schools purchase a wide variety of equipment, including IT equipment, such as interactive displays and desktop computers, as well as highly portable items, such as monitors, laptops and tablets.
  - These assets can make up a significant portion of a local government or school IT asset inventory, in both value and number.

Asset Inventories

Why Is It Important? (cont.)

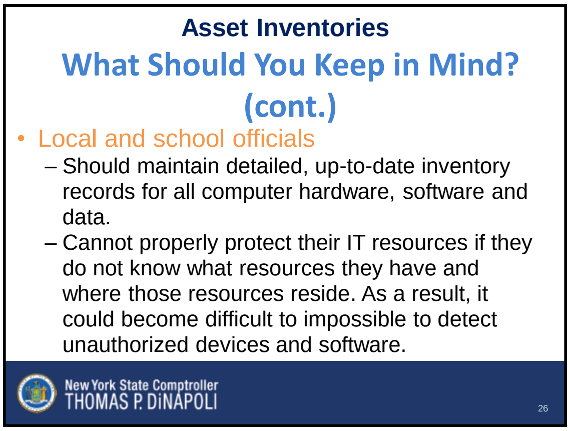
- As such, local and school officials are responsible for establishing governance over asset inventories.
- IT asset inventory oversight is a key aspect of **cybersecurity governance** to provide oversight and be cognizant of risks to these assets as they are subject to risks of loss, misuse and/or obsolescence.



Asset Inventories

What Should You Keep in Mind?

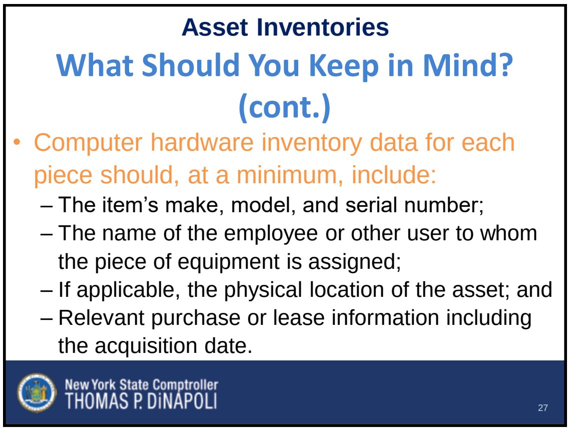
- The types of safekeeping policies and procedures used should address the risks associated with the assets being protected.
  - For example, some assets by their very nature may need more protection than others (e.g., mobile devices, laptop computers).
- Officials should verify the accuracy of IT asset inventory records through annual physical inventory counts.



Asset Inventories

What Should You Keep in Mind? (cont.)

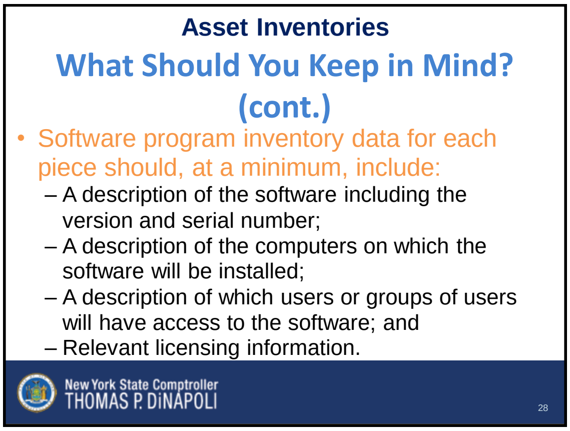
- Local and school officials
  - Should maintain detailed, up-to-date inventory records for all computer hardware, software and data.
  - Cannot properly protect their IT resources if they do not know what resources they have and where those resources reside. As a result, it could become difficult to impossible to detect unauthorized devices and software.



Asset Inventories

What Should You Keep in Mind? (cont.)

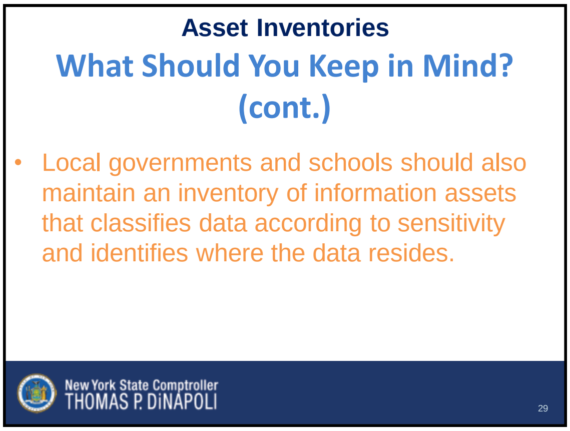
- Computer hardware inventory data for each piece should, at a minimum, include:
  - The item’s make, model, and serial number;
  - The name of the employee or other user to whom the piece of equipment is assigned;
  - If applicable, the physical location of the asset; and
  - Relevant purchase or lease information including the acquisition date.



Asset Inventories

What Should You Keep in Mind? (cont.)

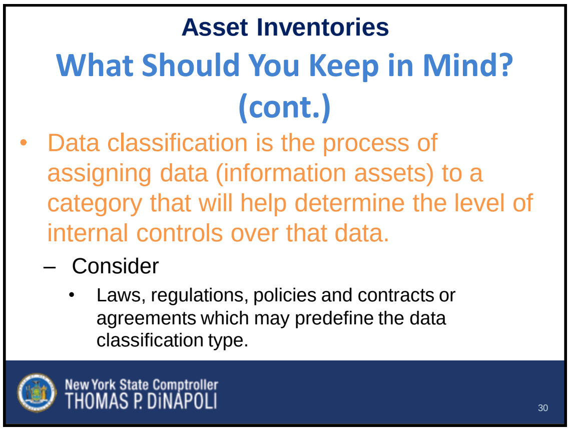
- Software program inventory data for each piece should, at a minimum, include:
  - A description of the software including the version and serial number;
  - A description of the computers on which the software will be installed;
  - A description of which users or groups of users will have access to the software; and
  - Relevant licensing information.



Asset Inventories

What Should You Keep in Mind? (cont.)

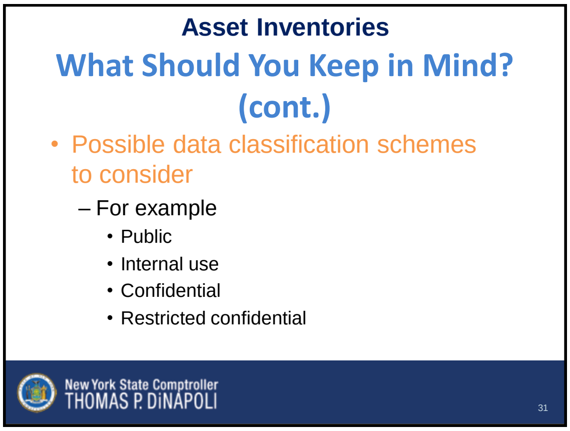
- Local governments and schools should also maintain an inventory of information assets that classifies data according to sensitivity and identifies where the data resides.



Asset Inventories

What Should You Keep in Mind? (cont.)

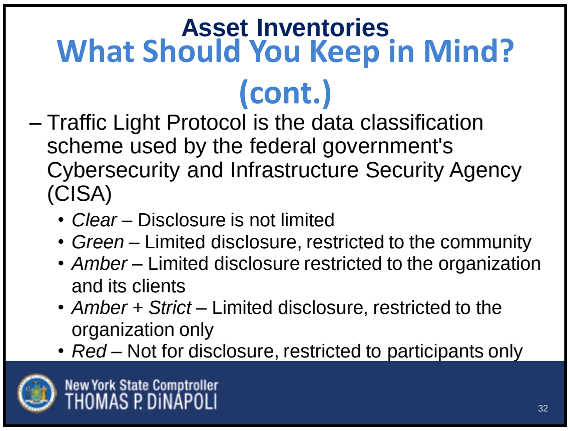
- Data classification is the process of assigning data (information assets) to a category that will help determine the level of internal controls over that data.
  - Consider
    - Laws, regulations, policies and contracts or agreements which may predefine the data classification type.



Asset Inventories

What Should You Keep in Mind? (cont.)

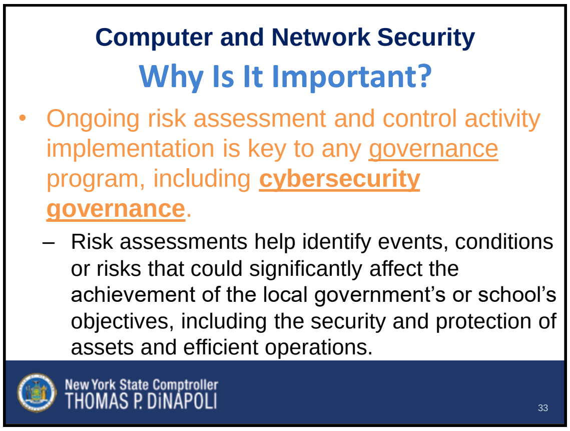
- Possible data classification schemes to consider
  - For example
    - Public
    - Internal use
    - Confidential
    - Restricted confidential



Asset Inventories

What Should You Keep in Mind? (cont.)

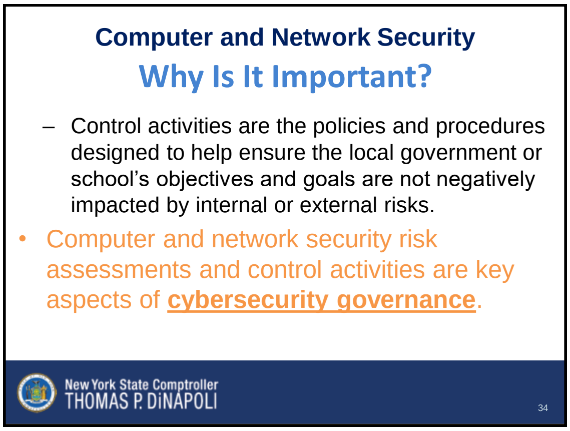
- Traffic Light Protocol is the data classification scheme used by the federal government's Cybersecurity and Infrastructure Security Agency (CISA)
  - *Clear* – Disclosure is not limited
  - *Green* – Limited disclosure, restricted to the community
  - *Amber* – Limited disclosure restricted to the organization and its clients
  - *Amber + Strict* – Limited disclosure, restricted to the organization only
  - *Red* – Not for disclosure, restricted to participants only



Computer and Network Security

Why Is It Important?

- Ongoing risk assessment and control activity implementation is key to any governance program, including **cybersecurity governance**.
  - Risk assessments help identify events, conditions or risks that could significantly affect the achievement of the local government's or school's objectives, including the security and protection of assets and efficient operations.

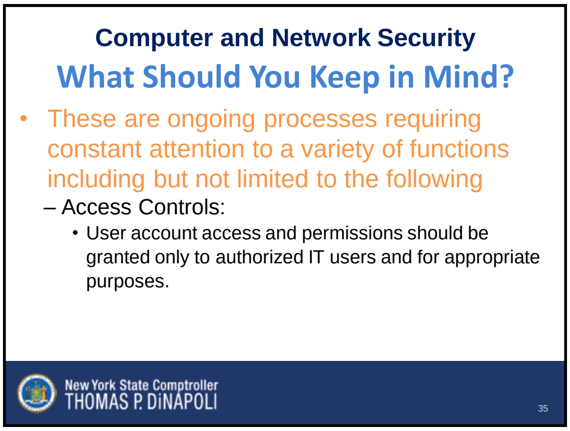


Computer and Network Security

Why Is It Important?

- Control activities are the policies and procedures designed to help ensure the local government or school’s objectives and goals are not negatively impacted by internal or external risks.

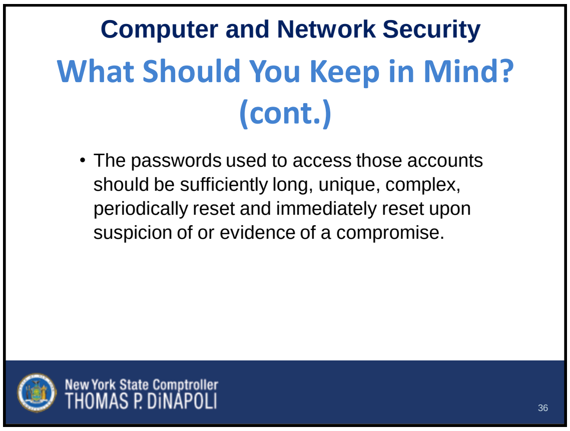
- Computer and network security risk assessments and control activities are key aspects of **cybersecurity governance**.



Computer and Network Security

What Should You Keep in Mind?

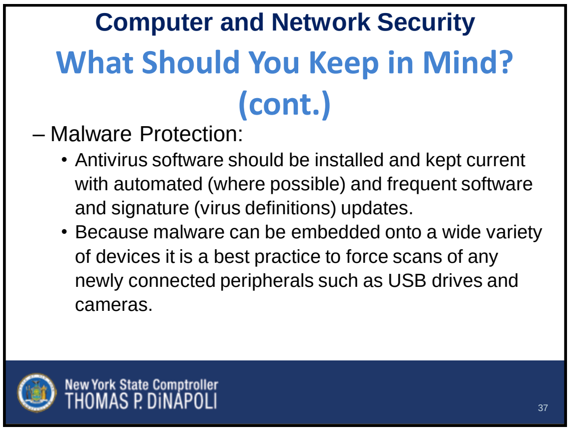
- These are ongoing processes requiring constant attention to a variety of functions including but not limited to the following
  - Access Controls:
    - User account access and permissions should be granted only to authorized IT users and for appropriate purposes.



Computer and Network Security

What Should You Keep in Mind? (cont.)

- The passwords used to access those accounts should be sufficiently long, unique, complex, periodically reset and immediately reset upon suspicion of or evidence of a compromise.



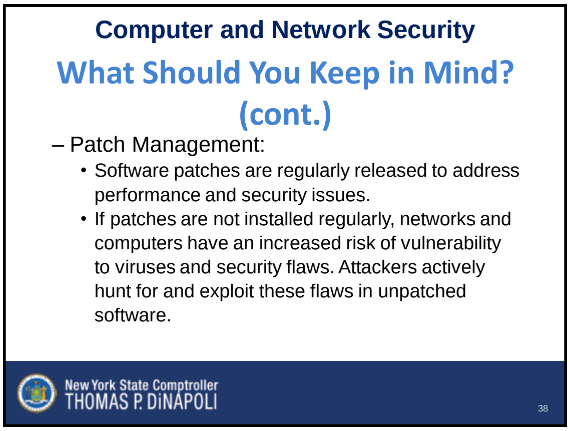
Computer and Network Security

What Should You Keep in Mind? (cont.)

- Malware Protection:
  - Antivirus software should be installed and kept current with automated (where possible) and frequent software and signature (virus definitions) updates.
  - Because malware can be embedded onto a wide variety of devices it is a best practice to force scans of any newly connected peripherals such as USB drives and cameras.

New York State Comptroller
THOMAS P. DiNAPOLI

37



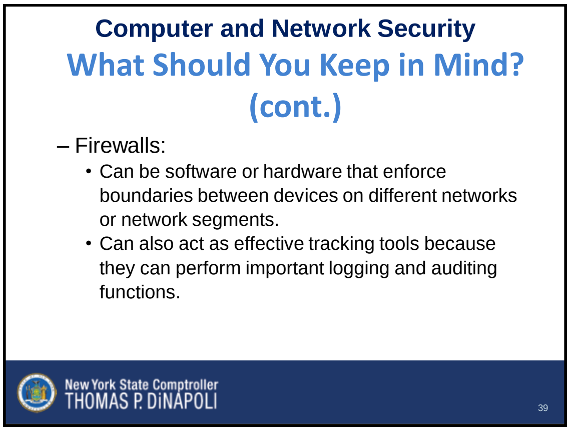
Computer and Network Security

What Should You Keep in Mind? (cont.)

- Patch Management:
  - Software patches are regularly released to address performance and security issues.
  - If patches are not installed regularly, networks and computers have an increased risk of vulnerability to viruses and security flaws. Attackers actively hunt for and exploit these flaws in unpatched software.

New York State Comptroller
THOMAS P. DiNAPOLI

38



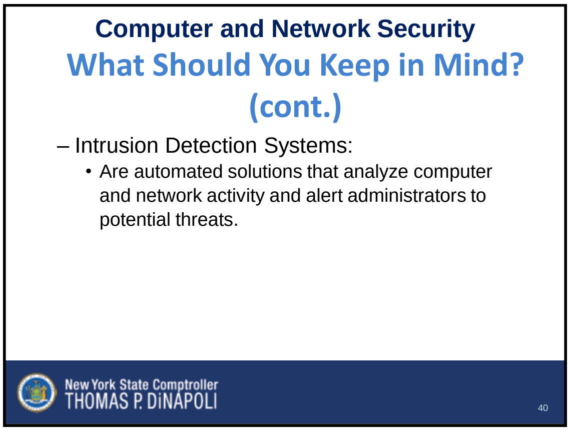
Computer and Network Security

What Should You Keep in Mind? (cont.)

- Firewalls:
  - Can be software or hardware that enforce boundaries between devices on different networks or network segments.
  - Can also act as effective tracking tools because they can perform important logging and auditing functions.

New York State Comptroller
THOMAS P. DiNAPOLI

39



Computer and Network Security

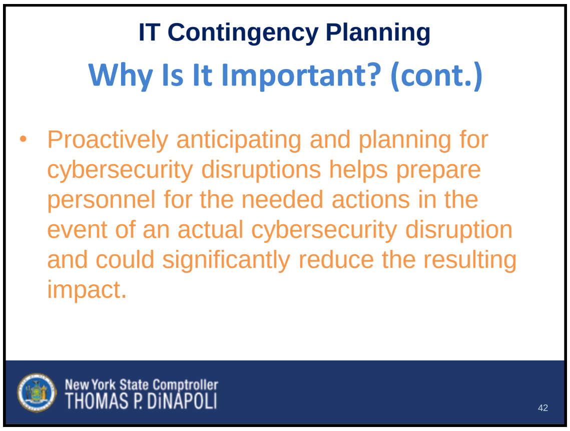
What Should You Keep in Mind? (cont.)

– Intrusion Detection Systems:
  - Are automated solutions that analyze computer and network activity and alert administrators to potential threats.

IT Contingency Planning

Why Is It Important?

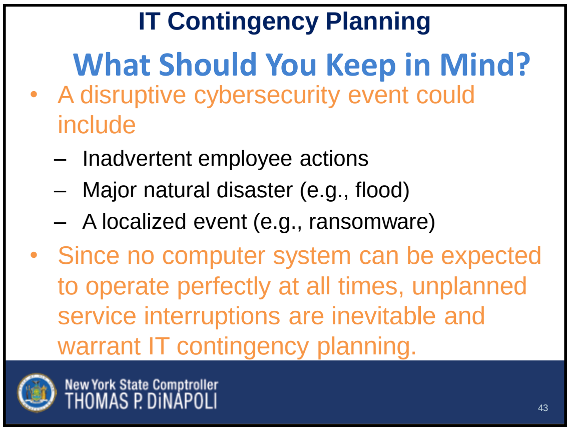
- Proactively planning for contingencies in the event of a disruption or emergencies is a key aspect of any governance program, including **cybersecurity governance**.
- IT contingency planning refers to the plans, policies, procedures and technical measures that help enable the recovery of IT operations after an unexpected incident.



IT Contingency Planning

Why Is It Important? (cont.)

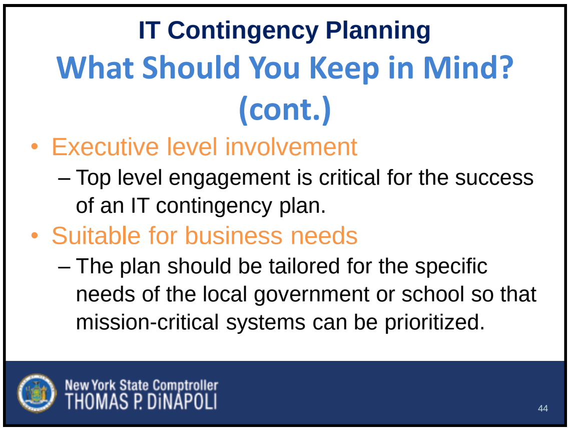
- Proactively anticipating and planning for cybersecurity disruptions helps prepare personnel for the needed actions in the event of an actual cybersecurity disruption and could significantly reduce the resulting impact.



IT Contingency Planning

What Should You Keep in Mind?

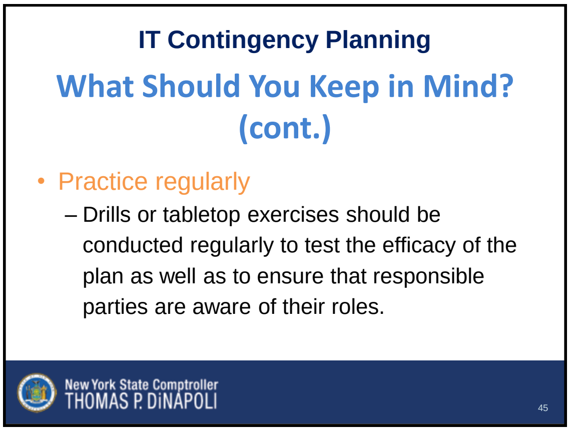
- A disruptive cybersecurity event could include
  - Inadvertent employee actions
  - Major natural disaster (e.g., flood)
  - A localized event (e.g., ransomware)
- Since no computer system can be expected to operate perfectly at all times, unplanned service interruptions are inevitable and warrant IT contingency planning.



IT Contingency Planning

What Should You Keep in Mind? (cont.)

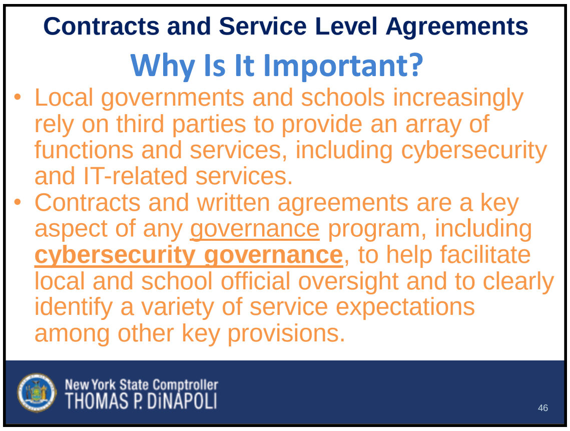
- Executive level involvement
  - Top level engagement is critical for the success of an IT contingency plan.
- Suitable for business needs
  - The plan should be tailored for the specific needs of the local government or school so that mission-critical systems can be prioritized.



IT Contingency Planning

What Should You Keep in Mind? (cont.)

- Practice regularly
  - Drills or tabletop exercises should be conducted regularly to test the efficacy of the plan as well as to ensure that responsible parties are aware of their roles.



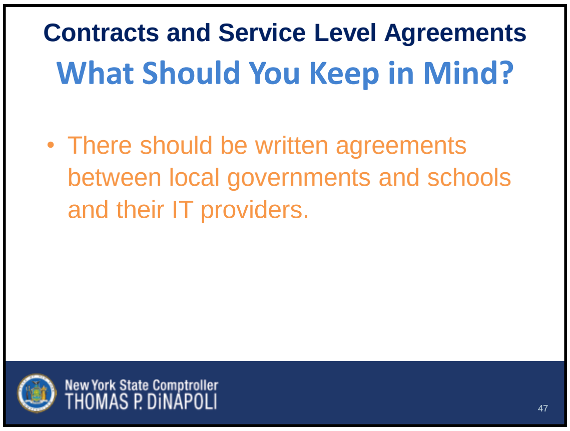
Contracts and Service Level Agreements

Why Is It Important?

- Local governments and schools increasingly rely on third parties to provide an array of functions and services, including cybersecurity and IT-related services.
- Contracts and written agreements are a key aspect of any governance program, including **cybersecurity governance**, to help facilitate local and school official oversight and to clearly identify a variety of service expectations among other key provisions.

New York State Comptroller
THOMAS P. DiNAPOLI

46



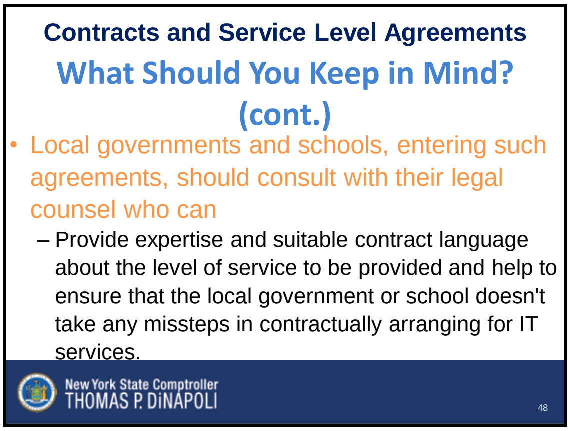
Contracts and Service Level Agreements

What Should You Keep in Mind?

- There should be written agreements between local governments and schools and their IT providers.

New York State Comptroller
THOMAS P. DiNAPOLI

47



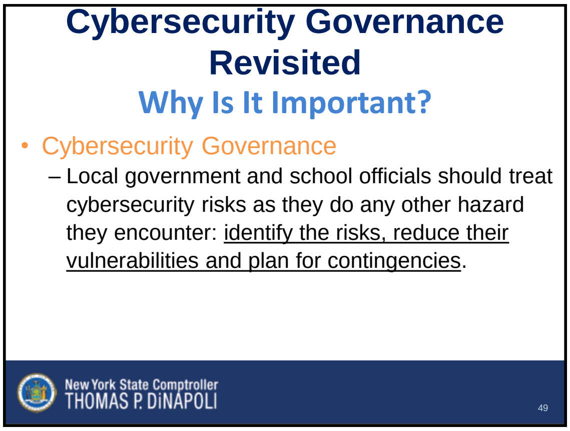
Contracts and Service Level Agreements

What Should You Keep in Mind? (cont.)

- Local governments and schools, entering such agreements, should consult with their legal counsel who can
  - Provide expertise and suitable contract language about the level of service to be provided and help to ensure that the local government or school doesn't take any missteps in contractually arranging for IT services.

New York State Comptroller
THOMAS P. DiNAPOLI

48

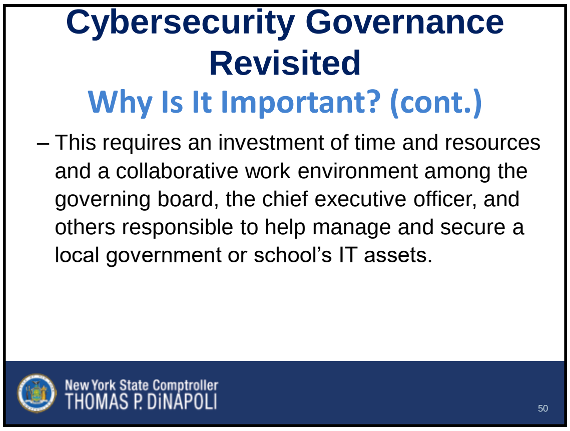


Cybersecurity Governance Revisited

Why Is It Important?

- Cybersecurity Governance
  - – 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.

New York State Comptroller
THOMAS P. DiNAPOLI

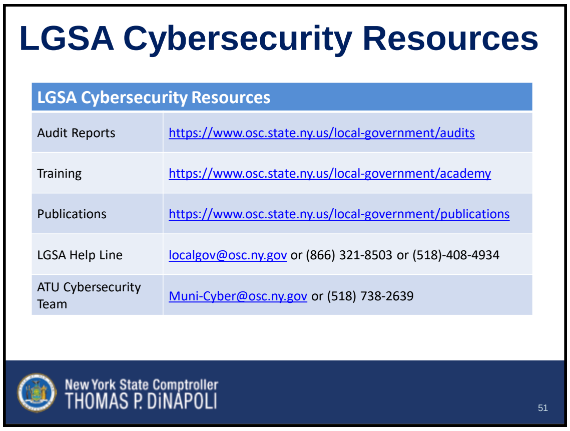


Cybersecurity Governance Revisited

Why Is It Important? (cont.)

– 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 or school's IT assets.

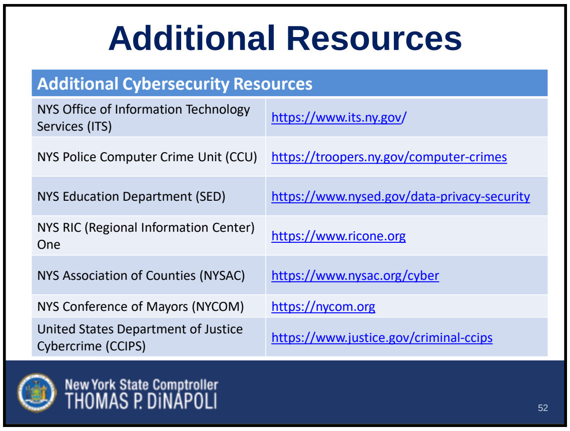
New York State Comptroller
THOMAS P. DiNAPOLI



LGSA Cybersecurity Resources

LGSA Cybersecurity Resources	
Audit Reports	https://www.osc.state.ny.us/local-government/audits
Training	https://www.osc.state.ny.us/local-government/academy
Publications	https://www.osc.state.ny.us/local-government/publications
LGSA Help Line	localgov@osc.ny.gov or (866) 321-8503 or (518)-408-4934
ATU Cybersecurity Team	Muni-Cyber@osc.ny.gov or (518) 738-2639

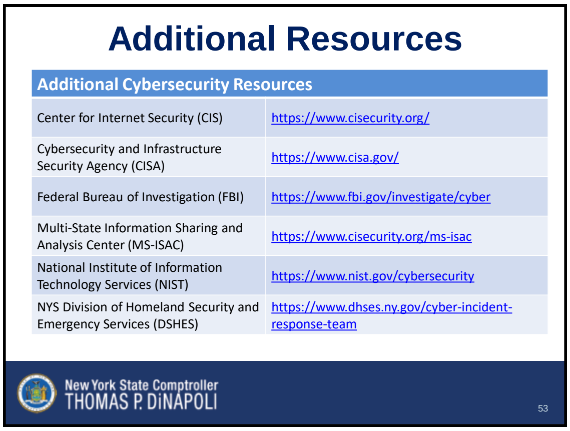
New York State Comptroller
THOMAS P. DiNAPOLI



Additional Resources

Additional Cybersecurity Resources	
NYS Office of Information Technology Services (ITS)	https://www.its.ny.gov/
NYS Police Computer Crime Unit (CCU)	https://troopers.ny.gov/computer-crimes
NYS Education Department (SED)	https://www.nysed.gov/data-privacy-security
NYS RIC (Regional Information Center) One	https://www.ricone.org
NYS Association of Counties (NYSAC)	https://www.nysac.org/cyber
NYS Conference of Mayors (NYCOM)	https://nycom.org
United States Department of Justice Cybercrime (CCIPS)	https://www.justice.gov/criminal-ccips

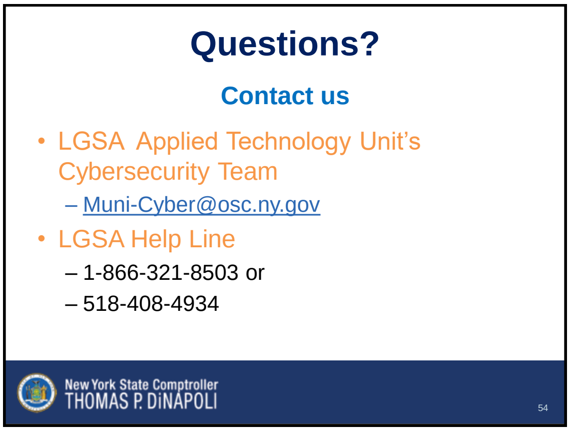
New York State Comptroller
THOMAS P. DiNAPOLI



Additional Resources

Additional Cybersecurity Resources	
Center for Internet Security (CIS)	https://www.cisecurity.org/
Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/
Federal Bureau of Investigation (FBI)	https://www.fbi.gov/investigate/cyber
Multi-State Information Sharing and Analysis Center (MS-ISAC)	https://www.cisecurity.org/ms-isac
National Institute of Information Technology Services (NIST)	https://www.nist.gov/cybersecurity
NYS Division of Homeland Security and Emergency Services (DSHES)	https://www.dhses.ny.gov/cyber-incident-response-team

New York State Comptroller
THOMAS P. DiNAPOLI

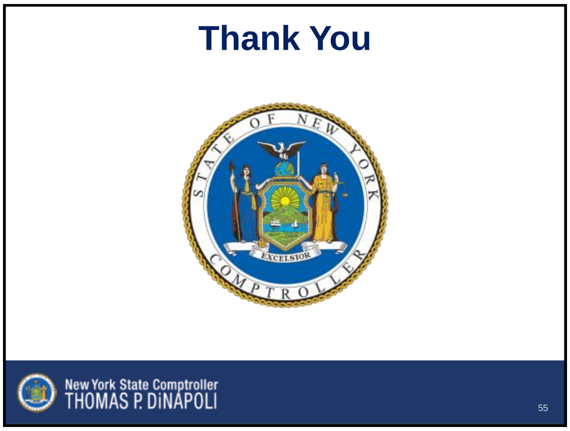


Questions?

Contact us

- LGSA Applied Technology Unit's Cybersecurity Team
  - Muni-Cyber@osc.ny.gov
- LGSA Help Line
  - 1-866-321-8503 or
  - 518-408-4934

New York State Comptroller
THOMAS P. DiNAPOLI



Thank You

New York State Comptroller
THOMAS P. DiNAPOLI

55