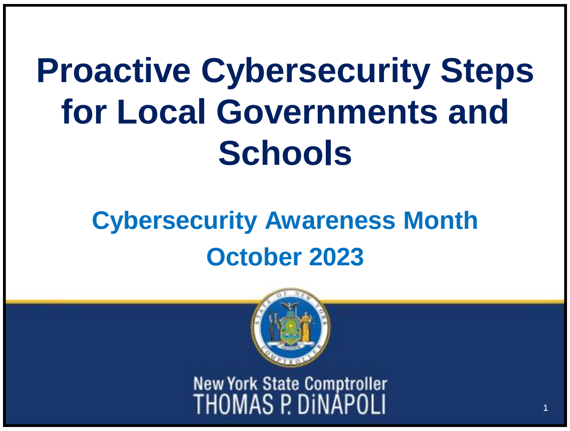
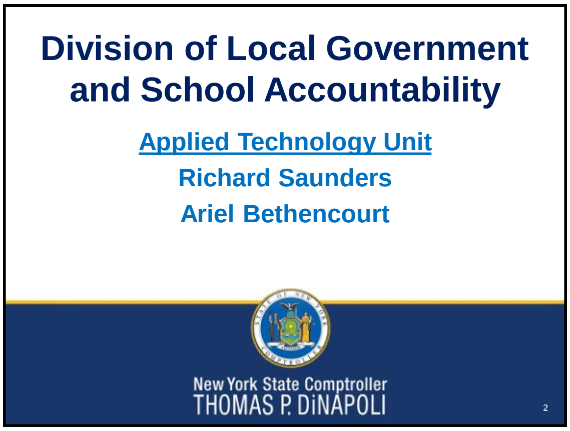


Proactive Cybersecurity Steps for Local Governments and Schools

Cybersecurity Awareness Month

October 2023

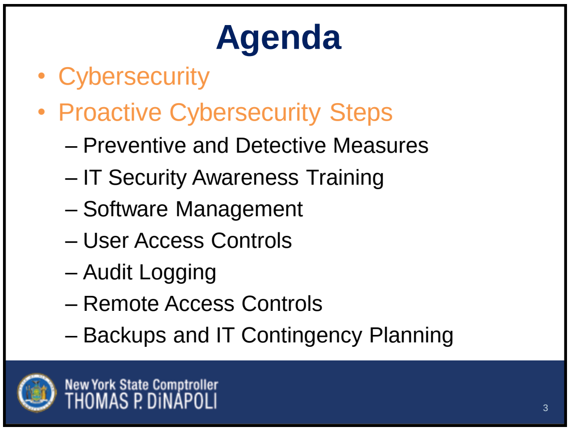


Division of Local Government and School Accountability

Applied Technology Unit

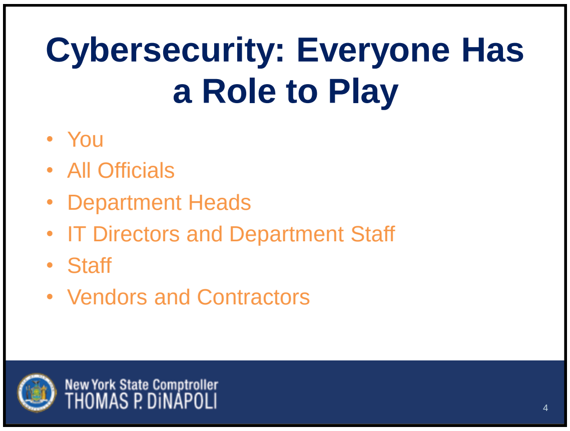
Richard Saunders

Ariel Bethencourt



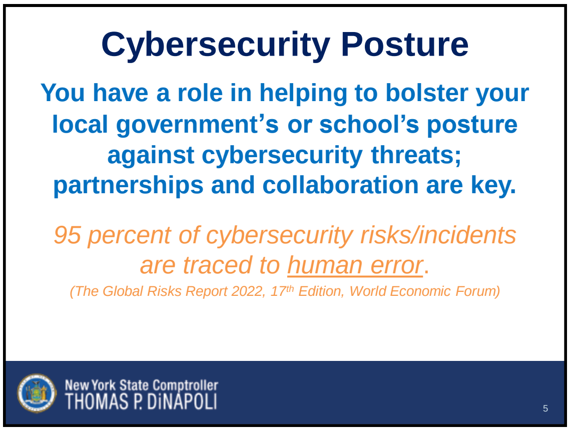
Agenda

- Cybersecurity
- Proactive Cybersecurity Steps
  - Preventive and Detective Measures
  - IT Security Awareness Training
  - Software Management
  - User Access Controls
  - Audit Logging
  - Remote Access Controls
  - Backups and IT Contingency Planning



Cybersecurity: Everyone Has a Role to Play

- You
- All Officials
- Department Heads
- IT Directors and Department Staff
- Staff
- Vendors and Contractors

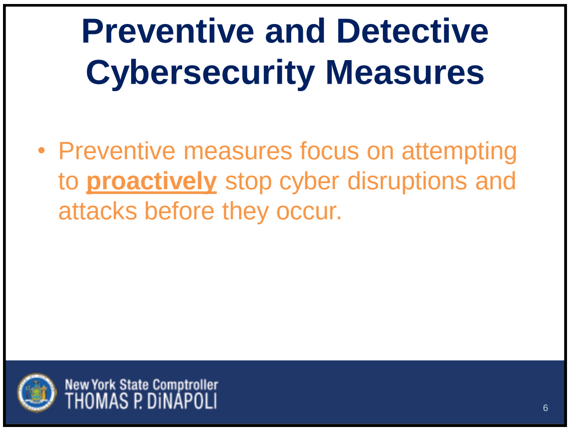


Cybersecurity Posture

You have a role in helping to bolster your local government's or school's posture against cybersecurity threats; partnerships and collaboration are key.

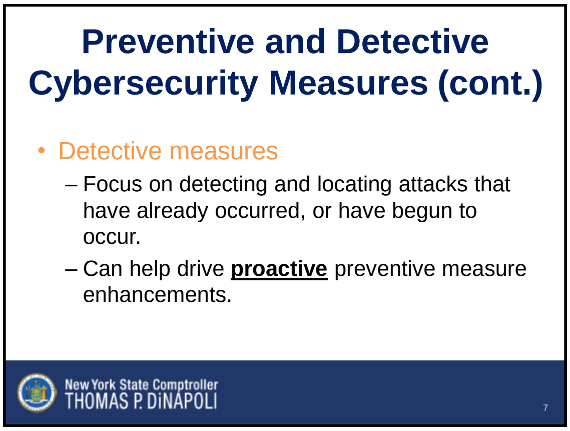
95 percent of cybersecurity risks/incidents are traced to human error.

(The Global Risks Report 2022, 17th Edition, World Economic Forum)



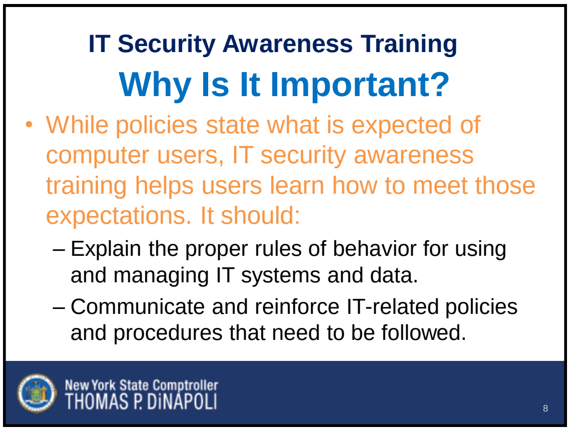
Preventive and Detective Cybersecurity Measures

- Preventive measures focus on attempting to **proactively** stop cyber disruptions and attacks before they occur.



Preventive and Detective Cybersecurity Measures (cont.)

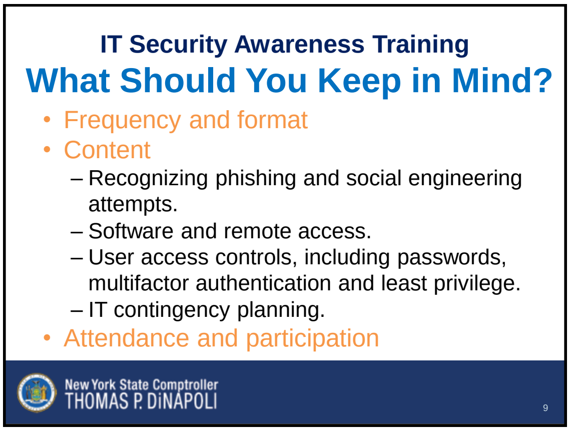
- Detective measures
  - Focus on detecting and locating attacks that have already occurred, or have begun to occur.
  - Can help drive **proactive** preventive measure enhancements.



IT Security Awareness Training

Why Is It Important?

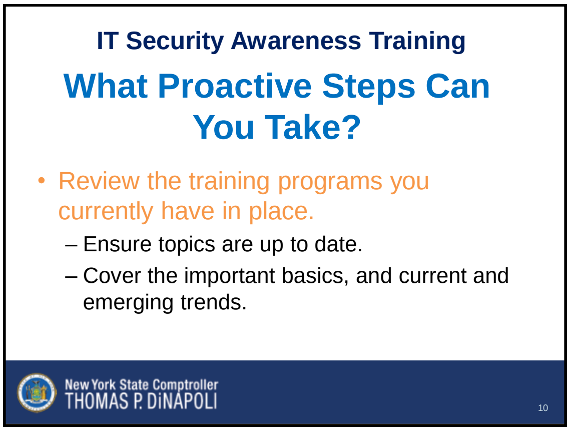
- While policies state what is expected of computer users, IT security awareness training helps users learn how to meet those expectations. It should:
  - Explain the proper rules of behavior for using and managing IT systems and data.
  - Communicate and reinforce IT-related policies and procedures that need to be followed.



IT Security Awareness Training

What Should You Keep in Mind?

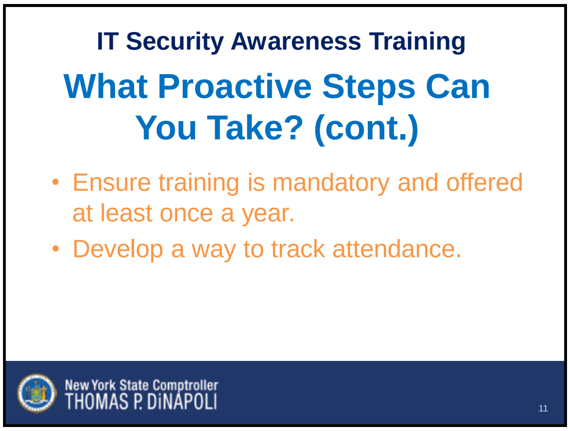
- Frequency and format
- Content
  - Recognizing phishing and social engineering attempts.
  - Software and remote access.
  - User access controls, including passwords, multifactor authentication and least privilege.
  - IT contingency planning.
- Attendance and participation



IT Security Awareness Training

What Proactive Steps Can You Take?

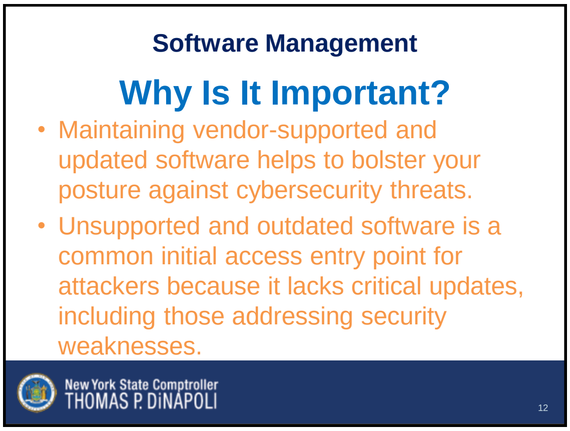
- Review the training programs you currently have in place.
  - Ensure topics are up to date.
  - Cover the important basics, and current and emerging trends.



IT Security Awareness Training

What Proactive Steps Can You Take? (cont.)

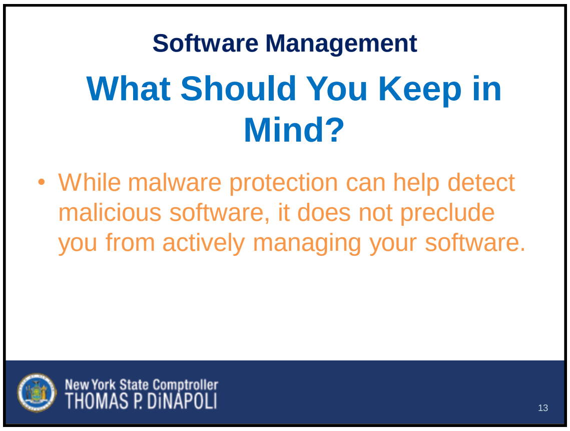
- Ensure training is mandatory and offered at least once a year.
- Develop a way to track attendance.



Software Management

Why Is It Important?

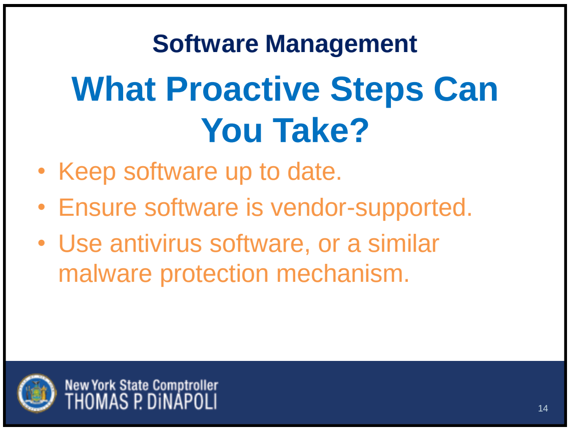
- Maintaining vendor-supported and updated software helps to bolster your posture against cybersecurity threats.
- Unsupported and outdated software is a common initial access entry point for attackers because it lacks critical updates, including those addressing security weaknesses.



Software Management

What Should You Keep in Mind?

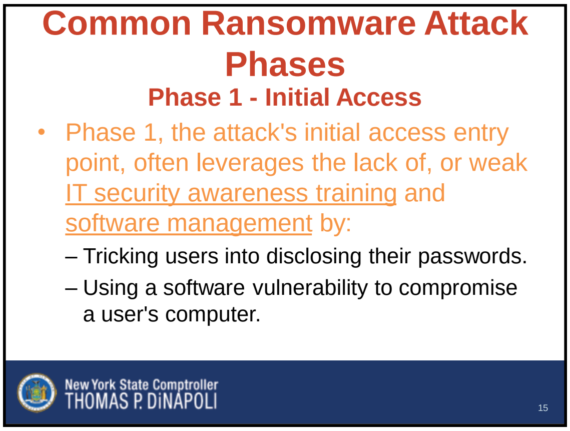
- While malware protection can help detect malicious software, it does not preclude you from actively managing your software.



Software Management

What Proactive Steps Can You Take?

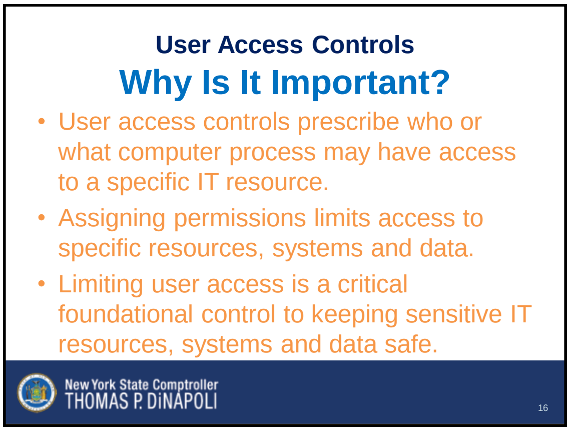
- Keep software up to date.
- Ensure software is vendor-supported.
- Use antivirus software, or a similar malware protection mechanism.



Common Ransomware Attack Phases

Phase 1 - Initial Access

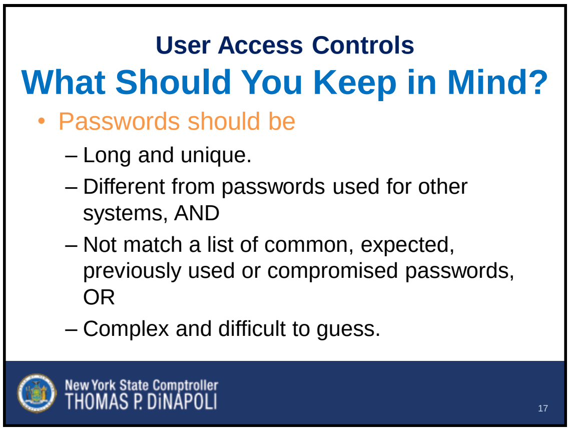
- Phase 1, the attack's initial access entry point, often leverages the lack of, or weak IT security awareness training and software management by:
  - – Tricking users into disclosing their passwords.
  - – Using a software vulnerability to compromise a user's computer.



User Access Controls

Why Is It Important?

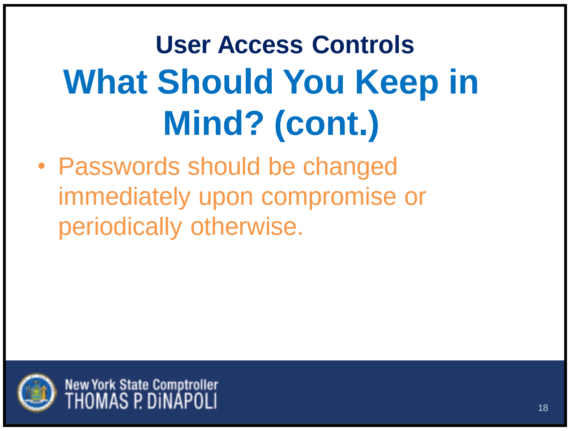
- User access controls prescribe who or what computer process may have access to a specific IT resource.
- Assigning permissions limits access to specific resources, systems and data.
- Limiting user access is a critical foundational control to keeping sensitive IT resources, systems and data safe.



User Access Controls

What Should You Keep in Mind?

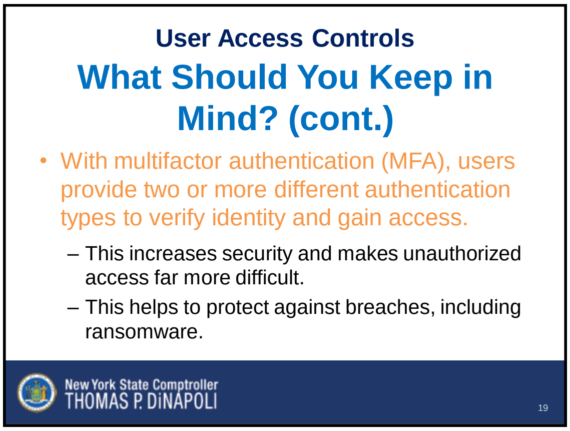
- Passwords should be
  - Long and unique.
  - Different from passwords used for other systems, AND
  - Not match a list of common, expected, previously used or compromised passwords, OR
  - Complex and difficult to guess.



User Access Controls

What Should You Keep in Mind? (cont.)

- Passwords should be changed immediately upon compromise or periodically otherwise.



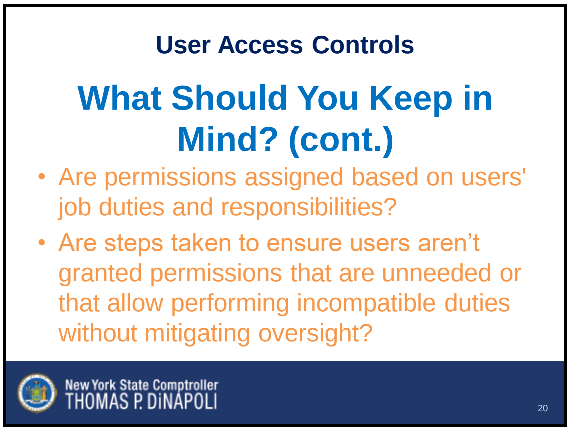
User Access Controls

What Should You Keep in Mind? (cont.)

- With multifactor authentication (MFA), users provide two or more different authentication types to verify identity and gain access.
  - – This increases security and makes unauthorized access far more difficult.
  - – This helps to protect against breaches, including ransomware.

New York State Comptroller
THOMAS P. DiNAPOLI

19



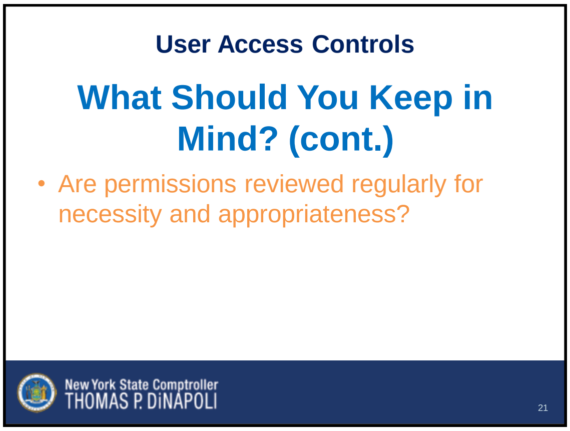
User Access Controls

What Should You Keep in Mind? (cont.)

- Are permissions assigned based on users' job duties and responsibilities?
- Are steps taken to ensure users aren’t granted permissions that are unneeded or that allow performing incompatible duties without mitigating oversight?

New York State Comptroller
THOMAS P. DiNAPOLI

20



User Access Controls

What Should You Keep in Mind? (cont.)

- Are permissions reviewed regularly for necessity and appropriateness?

New York State Comptroller
THOMAS P. DiNAPOLI

21

User Access Controls

What Proactive Steps Can You Take?

- Enforce strong password requirements.
- Implement MFA for administrative, remote and other key user access.
- Remove unneeded access in a timely manner.

Common Ransomware Attack Phases

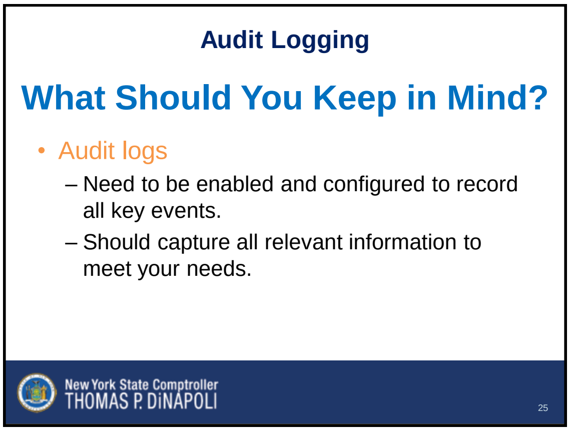
Phase 2 - Gained Foothold

- Phase 2, the attack's gained access or foothold, often leverages lacking or weak user access controls by:
  - Exploring initial access and escalation potential.
  - Determining ransomware infection initiation capabilities.

Audit Logging

Why Is It Important?

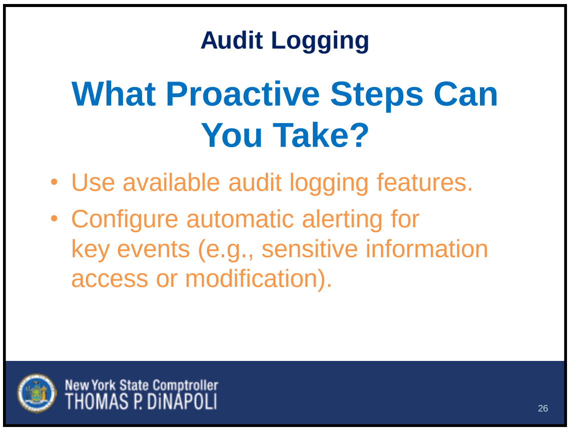
- Audit logs contain information for events that happen within networks, systems, and software.
- Audit logs can help determine:
  - Who accessed data or systems.
  - What data or systems were accessed.
  - When the data or systems were accessed.
  - Where data or systems were changed.



Audit Logging

What Should You Keep in Mind?

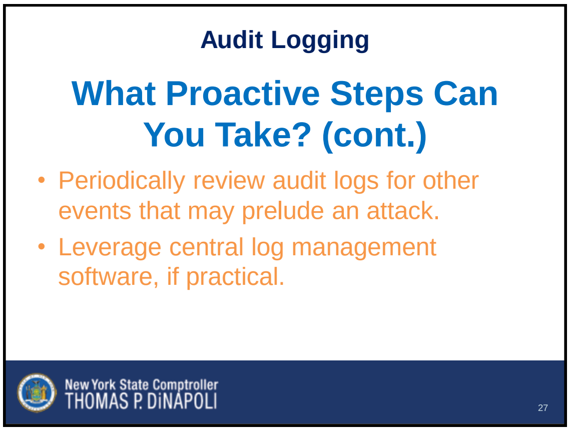
- Audit logs
  - Need to be enabled and configured to record all key events.
  - Should capture all relevant information to meet your needs.



Audit Logging

What Proactive Steps Can You Take?

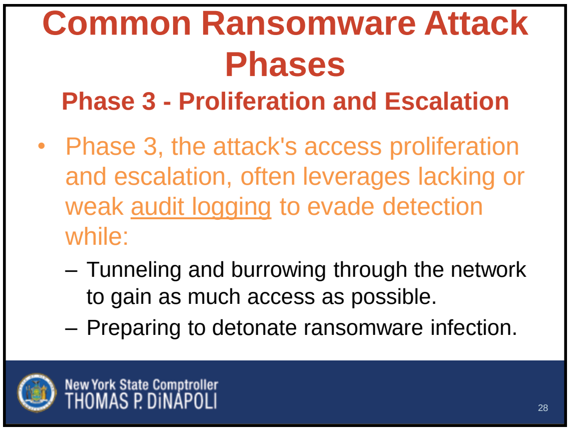
- Use available audit logging features.
- Configure automatic alerting for key events (e.g., sensitive information access or modification).



Audit Logging

What Proactive Steps Can You Take? (cont.)

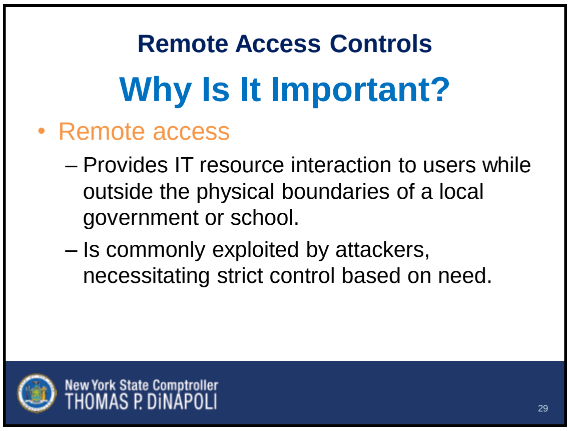
- Periodically review audit logs for other events that may prelude an attack.
- Leverage central log management software, if practical.



Common Ransomware Attack Phases

Phase 3 - Proliferation and Escalation

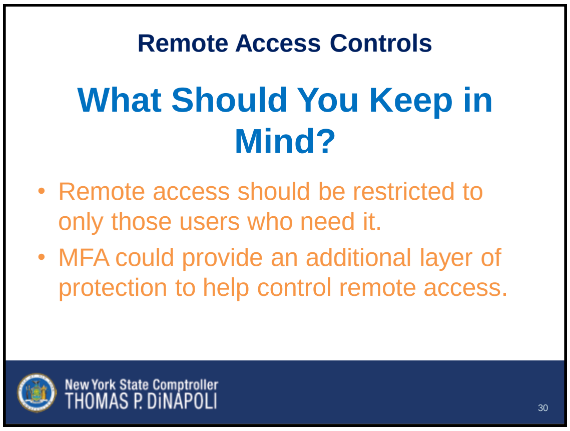
- Phase 3, the attack's access proliferation and escalation, often leverages lacking or weak audit logging to evade detection while:
  - Tunneling and burrowing through the network to gain as much access as possible.
  - Preparing to detonate ransomware infection.



Remote Access Controls

Why Is It Important?

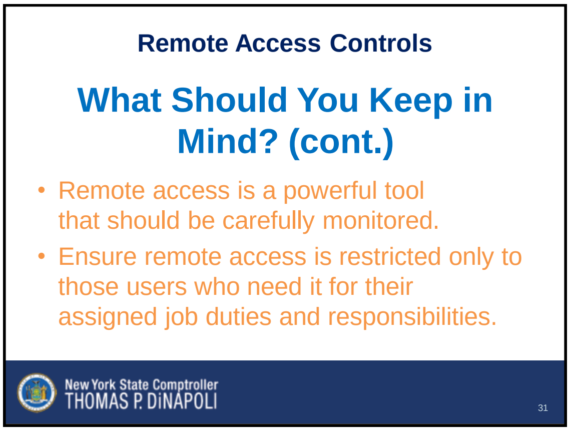
- Remote access
  - Provides IT resource interaction to users while outside the physical boundaries of a local government or school.
  - Is commonly exploited by attackers, necessitating strict control based on need.



Remote Access Controls

What Should You Keep in Mind?

- Remote access should be restricted to only those users who need it.
- MFA could provide an additional layer of protection to help control remote access.

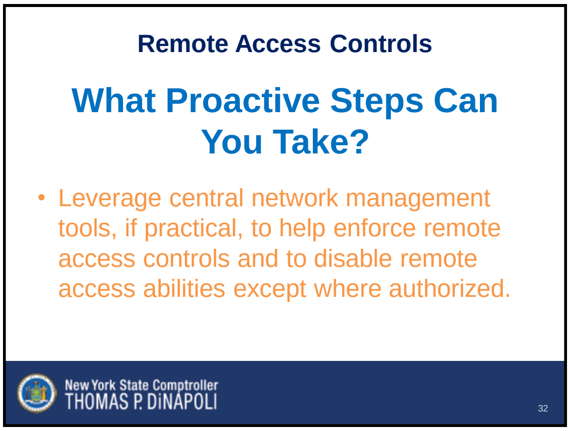


Remote Access Controls

What Should You Keep in Mind? (cont.)

- Remote access is a powerful tool that should be carefully monitored.
- Ensure remote access is restricted only to those users who need it for their assigned job duties and responsibilities.

New York State Comptroller
THOMAS P. DiNAPOLI

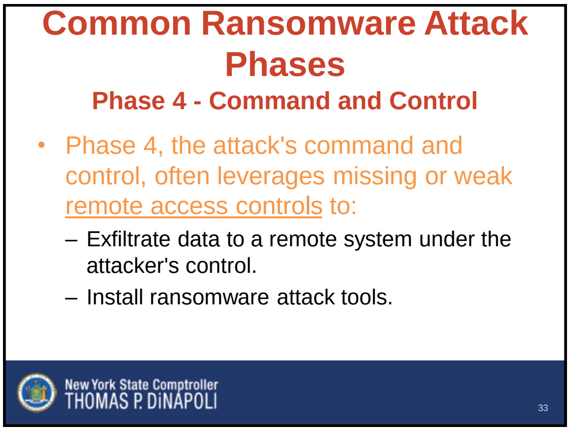


Remote Access Controls

What Proactive Steps Can You Take?

- Leverage central network management tools, if practical, to help enforce remote access controls and to disable remote access abilities except where authorized.

New York State Comptroller
THOMAS P. DiNAPOLI

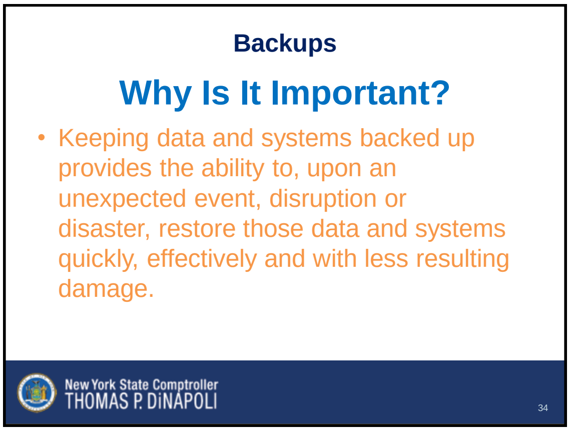


Common Ransomware Attack Phases

Phase 4 - Command and Control

- Phase 4, the attack's command and control, often leverages missing or weak remote access controls to:
  - Exfiltrate data to a remote system under the attacker's control.
  - Install ransomware attack tools.

New York State Comptroller
THOMAS P. DiNAPOLI



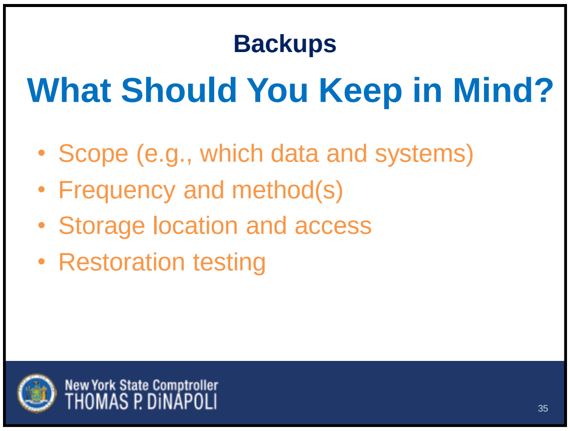
Backups

Why Is It Important?

- Keeping data and systems backed up provides the ability to, upon an unexpected event, disruption or disaster, restore those data and systems quickly, effectively and with less resulting damage.

New York State Comptroller
THOMAS P. DiNAPOLI

34



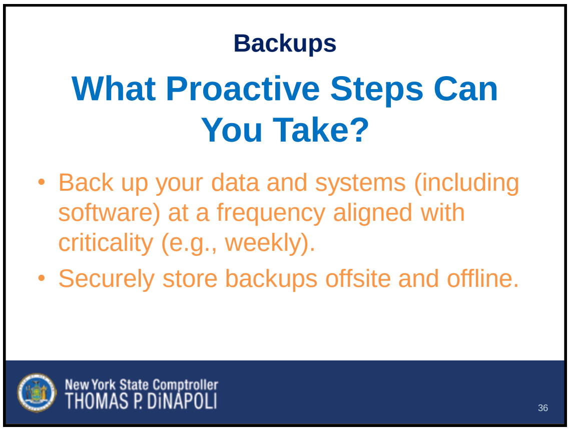
Backups

What Should You Keep in Mind?

- Scope (e.g., which data and systems)
- Frequency and method(s)
- Storage location and access
- Restoration testing

New York State Comptroller
THOMAS P. DiNAPOLI

35



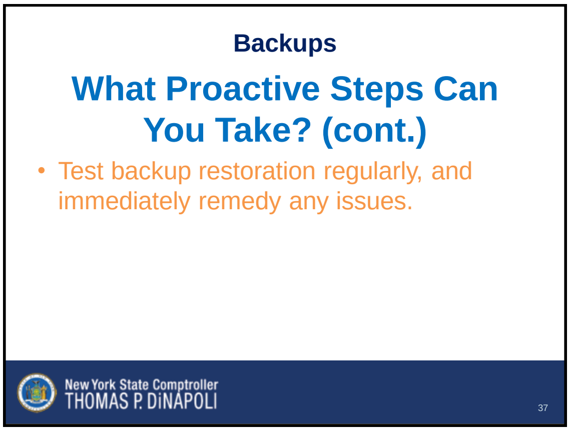
Backups

What Proactive Steps Can You Take?

- Back up your data and systems (including software) at a frequency aligned with criticality (e.g., weekly).
- Securely store backups offsite and offline.

New York State Comptroller
THOMAS P. DiNAPOLI

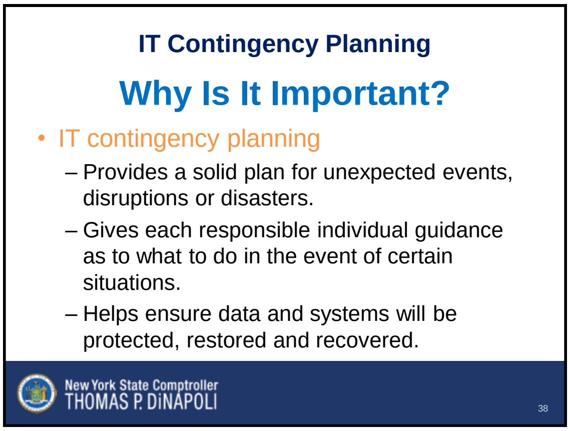
36



Backups

What Proactive Steps Can You Take? (cont.)

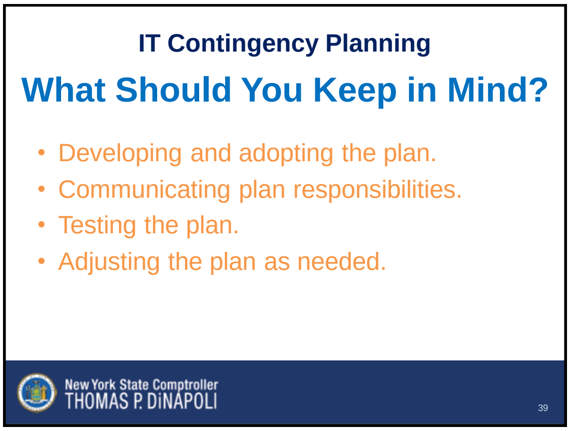
- Test backup restoration regularly, and immediately remedy any issues.



IT Contingency Planning

Why Is It Important?

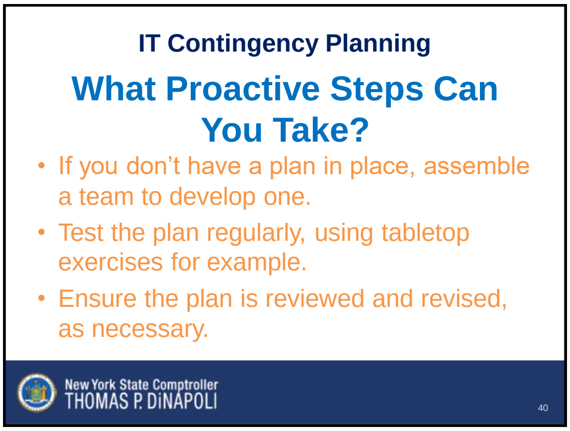
- IT contingency planning
  - – Provides a solid plan for unexpected events, disruptions or disasters.
  - – Gives each responsible individual guidance as to what to do in the event of certain situations.
  - – Helps ensure data and systems will be protected, restored and recovered.



IT Contingency Planning

What Should You Keep in Mind?

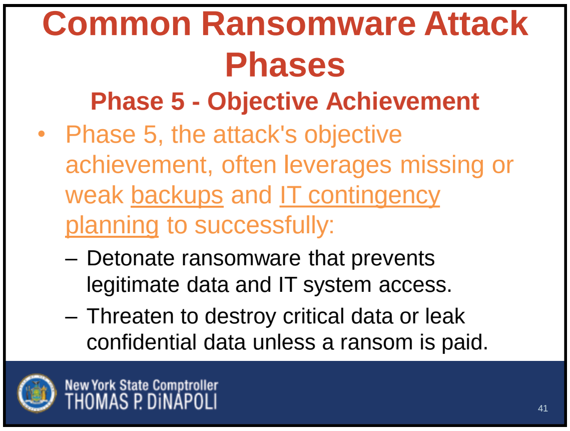
- Developing and adopting the plan.
- Communicating plan responsibilities.
- Testing the plan.
- Adjusting the plan as needed.



IT Contingency Planning

What Proactive Steps Can You Take?

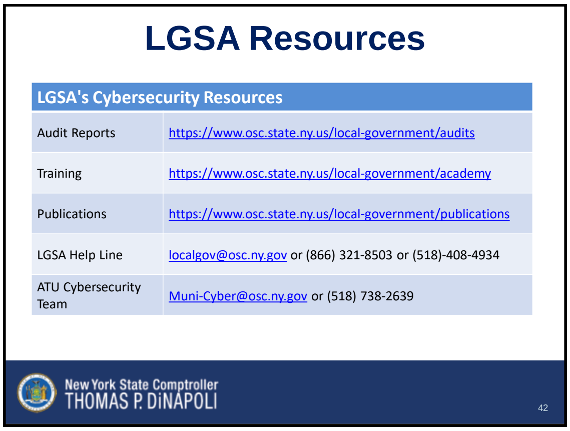
- If you don't have a plan in place, assemble a team to develop one.
- Test the plan regularly, using tabletop exercises for example.
- Ensure the plan is reviewed and revised, as necessary.



Common Ransomware Attack Phases

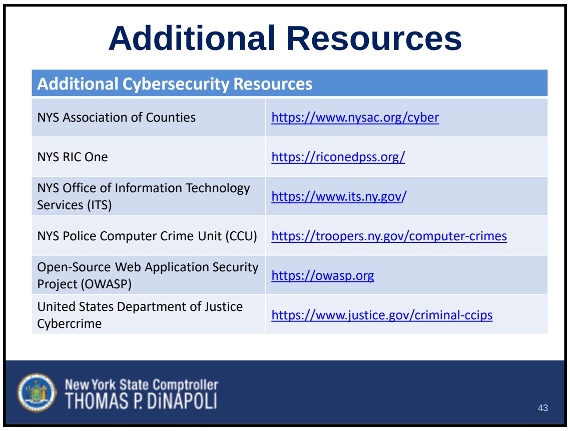
Phase 5 - Objective Achievement

- Phase 5, the attack's objective achievement, often leverages missing or weak backups and IT contingency planning to successfully:
  - Detonate ransomware that prevents legitimate data and IT system access.
  - Threaten to destroy critical data or leak confidential data unless a ransom is paid.



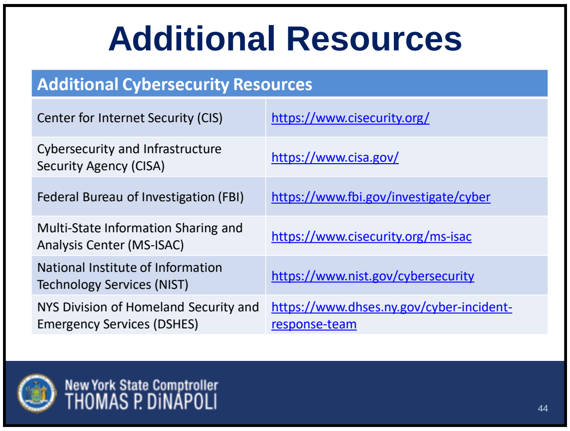
LGSA Resources

LGSA's 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



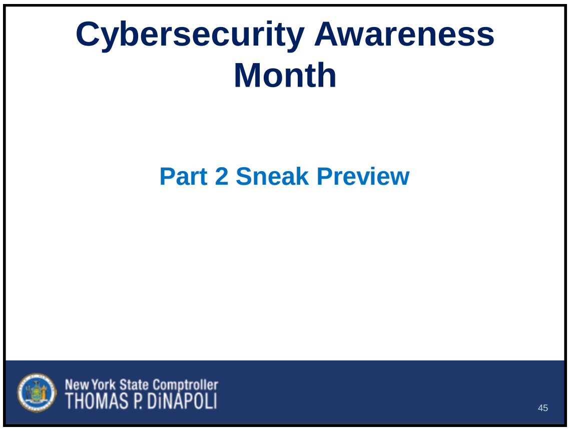
Additional Resources

Additional Cybersecurity Resources	
NYS Association of Counties	https://www.nysac.org/cyber
NYS RIC One	https://riconedpss.org/
NYS Office of Information Technology Services (ITS)	https://www.its.ny.gov/
NYS Police Computer Crime Unit (CCU)	https://troopers.ny.gov/computer-crimes
Open-Source Web Application Security Project (OWASP)	https://owasp.org
United States Department of Justice Cybercrime	https://www.justice.gov/criminal-ccips



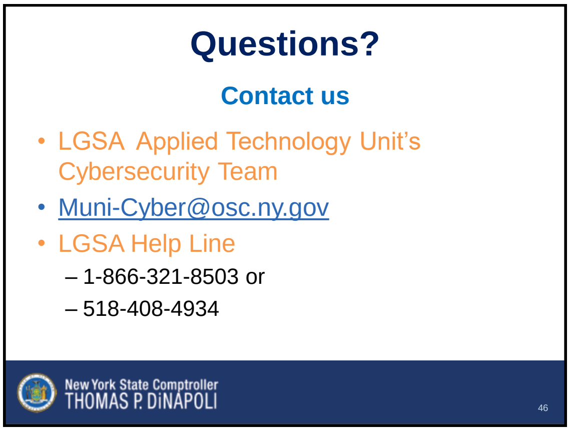
Additional Resources

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



Cybersecurity Awareness Month

Part 2 Sneak Preview



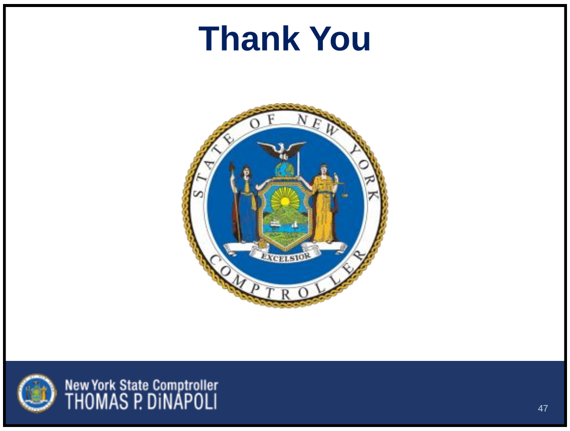
Questions?

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

46



Thank You

New York State Comptroller
THOMAS P. DiNAPOLI

47