



## Presentation Objectives

Improve the cybersecurity of local governments by:

- Reviewing cybersecurity fundamentals.
- Raising awareness about cybersecurity best practices.
- Describing common cybersecurity threats and ways to reduce the risk of becoming a victim.
- Encouraging and enabling participants to evaluate their cybersecurity policies, procedures and technologies.





## Cybersecurity Fundamentals



## What are you protecting data from?


- Accidental disclosure of personal, private or sensitive information
  - Access controls
  - Public website
  - Disposal
- Theft
  - Insider Threat
  - External Threat
- Loss
  - Accidental
  - Disaster (e.g., computer virus; flood)



## Hackers, Attackers and Individuals with Malicious Intent


Regardless of what you call them – hackers, attackers or individuals with malicious intent – there are people who may intentionally try to access your computers and data without authorization.

- Looking for profit, enjoyment, payback or a challenge.
- Possessing expert technical skill or very little skill.
- Seeking specific targets or crimes of opportunity.
- Originating from inside or outside of the entity.



## Cybersecurity Defined

- The body of technologies, processes, and practices designed to protect computers, networks, programs, and data from attack, damage, or unauthorized access.
- One of the most challenging aspects of cybersecurity is the quickly and constantly evolving nature of security risks.



## A Realistic Assumption

Somewhere out in cyberspace there is a hacker, attacker or individual with malicious intent who would like to harm, steal, access, sell, and/or disrupt your computer system, website and/or electronic data.

- It is no longer wise to think that nobody is interested in your computers, network or data, because you are too small or don't have anything of value to steal.
- History has shown that cybercrimes sometimes affect the most unlikely victims.

NSA COMPTROLLER  
THOMAS P. DINAPOLI

## IT Risk Assessment

- Potential loss of the confidentiality, integrity and/or availability (CIA) of electronic information or IT systems.
- Extent to which an organization is threatened by a potential IT security circumstance or event.
  - Function of both the adverse impacts that would arise if the circumstance or event occurs and the likelihood of such occurrence.
- IT risk assessment a sound starting point for determining what can threaten the safety and security of your IT environment and then developing a strategy for addressing those threats.

NSA COMPTROLLER  
THOMAS P. DINAPOLI

## IT Security Fundamentals: CIA Triad

- CIA Triad: An IT security model comprising three main components: confidentiality, integrity and availability (CIA). Each component represents a fundamental objective of information security.



- **Confidentiality:** To ensure that information is confidential, it must be organized in terms of its sensitivity and who should have access to the data.
- **Integrity:** To ensure its integrity, the information must be accurate and complete.
- **Availability:** To ensure its availability, the information must be ready for access at whatever time it is needed.

NSA COMPTROLLER  
THOMAS P. DINAPOLI

## IT Security Fundamentals: Defense-in-Depth

**Defense-in-depth:** The implementation of multiple layers of security at strategic points in the IT infrastructure to protect data, networks and computer systems.

A combination of controls:

- Helps ensure that your system does not become overly dependent on any one control; and
- Provides added protection in case a layer of security fails to function properly or does not detect or stop a threat to your data.

*There is no single control that can be used to adequately protect against today's sophisticated threats; only a combination of multiple preventive and detective controls will keep your data and systems safe.*

NSA COMPTROLLER  
THOMAS P. DINAPOLI

## IT Security Fundamentals: Strictly Control the Use of Administrative Privileges

**Administrative privileges** are highly privileged accounts that generally allow users to: view all data on the system or network; make changes to the settings configured on the system or network; and create new user accounts, or change the levels of privileges granted to existing user accounts, on the system or network.

Administrative privileges are necessary for only a *small number* of users with particular job duties.

There are countless ways that attackers who gain administrative privileges can leverage their positions to increase the level of damage caused when a system or network is breached.

NSA COMPTROLLER  
THOMAS P. DINAPOLI

## Cybersecurity Best Practices

NSA COMPTROLLER  
THOMAS P. DINAPOLI

## No-cost or Low-cost Solutions

Audits often identify significant weaknesses in local governments' IT governance (e.g., the adoption and distribution of policies and plans) and basic technical controls.

Most OSC recommendations to improve these issues are **no-cost or low-cost solutions**.

- For example, while most of the computer systems have some electronic means to provide security (e.g., limit access to data and systems, produce logs that contain valuable information), local government personnel do not always use these built-in tools.

NEW YORK STATE OFFICE OF  
THOMAS P. DINAPOLI

## IT Security Top Twelve

- IT Policies
- Cybersecurity Training
- Computer Hardware, Software, and Data Inventories
- Contracts for IT Services
- Virus Protection
- Patch Management
- Access Controls
- Online Banking Controls
- Wireless Networks
- Firewalls and Intrusion Detection Systems
- Physical Controls
- Service Continuity and Disaster Recovery

NEW YORK STATE OFFICE OF  
THOMAS P. DINAPOLI

## Policies and Procedures

**Best Practice:** Adopt IT policies that define appropriate user behavior, describe the tools and procedures needed to protect data and information systems, and explain the consequences of policy violations. Provide organization-wide, cybersecurity training that is closely tied to the IT policies.

- Acceptable Use
- Mobile Devices
- Breach Notification (New York State Technology Law Section 208 (8))
- Passwords
- Online Banking

While your IT policies tell users what to do, training provides them with the skills to do it.

NEW YORK STATE OFFICE OF  
THOMAS P. DINAPOLI

## IT Awareness Training

- A well-informed work force is the strongest link in the chain to secure electronic data and computer systems.
- People who use and manage electronic data must understand policies, procedures and their roles in data security.
- Training should explain the proper rules of behavior (e.g., acceptable use).
- Distribute security reminders and alerts to reinforce training and policies.
- Focus on IT security in general or some narrow aspect of security (e.g., the danger of opening an email attachment from an unknown source).

NEW YORK STATE OFFICE OF  
THOMAS P. DINAPOLI

## Sources for Free or Low-Cost Cybersecurity Training

Center for Internet Security  
<https://www.cisecurity.org/>

New York State Office of Information Technology Services  
<https://www.its.ny.gov/>

New York State Office of the State Comptroller  
<http://www.osc.state.ny.us/>

TEEX Domestic Preparedness Campus  
<https://teex.org/Pages/homeland-security.aspx>

United States Computer Emergency Readiness Team  
<https://www.us-cert.gov/>

NEW YORK STATE OFFICE OF  
THOMAS P. DINAPOLI

## Most Important Cybersecurity Control

You 😊

- An individual who is vigilant about cybersecurity can have a significant, positive impact on the cybersecurity of an organization through the early identification of potential computer problems.
- A screen looks different, a task takes unusually long or an unfamiliar message requesting an action or information appears.
- Check with IT support personnel before clicking on any attachment or link that is suspicious, unexpected or confusing.

NEW YORK STATE OFFICE OF  
THOMAS P. DINAPOLI

## Cybersecurity Threat: Phishing

A social-engineering method in which the attacker sends out legitimate-looking emails to many individuals at once, in an attempt to gather confidential information (e.g., online banking passwords) from victims.

Why is phishing so successful?

- Many organizations fail to provide their computer users with cybersecurity training.
  - **Without cybersecurity training and awareness efforts, an organization's computer users are too quick to open emails from unknown senders, open attachments and click on links.**

408 COMPUTER ILLER  
THOMAS P. DINAPOLI

## Hardware, Software and Data Inventories

**Best Practice:** Maintain detailed, up-to-date inventory records for all computer hardware, software and electronic data.

Without the proper identification of all devices on a network, unauthorized devices and software can be easily introduced, putting the network and data at risk. A single compromised device can become a launching point for further network attacks, quickly turning one compromised device into many.

Inadequate inventory records makes it unlikely that software patches necessary to address known security vulnerabilities can be applied on a timely basis, if at all.

408 COMPUTER ILLER  
THOMAS P. DINAPOLI

## Hardware, Software and Data Inventories

(Continued)

Inadequate records increases the likelihood that you may inadvertently violate copyright laws by having more software users than licenses for a particular application and incur penalties as a result.

IT security alerts and bulletins issued by software vendors, municipal associations, and federal and state agencies reference specific types and versions of devices and software. These alerts are intended to raise awareness about threats, sometimes imminent threats, to computer systems. Accurate inventory records can help you determine if these advisories are relevant to your unique computing environment.

It is very challenging to protect computer resources, including data, if you do not know exactly what resources you have and where those resources reside.

408 COMPUTER ILLER  
THOMAS P. DINAPOLI

## Data Classification

Data classification is the process of assigning data to a category (e.g., public, internal use, confidential) that will determine the level of internal controls over that data.

An inventory of information assets (i.e., data) that classifies data according to its sensitivity and identifies where the data resides (e.g., servers, workstations, and laptops) is important because different kinds of information require different levels of protection.

**Example:** Where are all the places that your organization stores dates of birth, names and social security numbers?

- Who has access to the information (principle of least privilege)?
- What are the controls over that information?

408 COMPUTER ILLER  
THOMAS P. DINAPOLI

## Data Classifications



**Data:** Data should be classified based on sensitivity, and the location of each type of data should be identified. An example of a data classification scheme follows:

<b>Public</b>	Widely available to all through publications, pamphlets, and web content.
<b>Internal</b>	Operational information not approved for general circulation.
<b>Confidential</b>	Information used in performing critical work or that may be used to identify an individual.
<b>Restricted</b>	Information where disclosure, loss, or unauthorized modification would have the most serious impact on the organization's ability to fulfill business responsibilities.

*You cannot properly protect data if you do not know what type of data you have, what form it is in (electronic, paper or both) and where it resides*

408 COMPUTER ILLER  
THOMAS P. DINAPOLI

## Data Inventory Overload

- Do not retain more data than necessary.
  - Costly to store and protect.
  - Excessive data increases data risks.
- Contact the New York State Archives for records retention guidance.  
<http://www.archives.nysed.gov/aindex.shtml>

408 COMPUTER ILLER  
THOMAS P. DINAPOLI

## Public Website Information Disclosure

**Best Practice:** Establish a framework for classifying data based on its level of sensitivity, review *all* materials *before* they are posted to your public website, and then periodically review the content of your public website to ensure that your internal controls over sensitive information are operating as intended.

Google search operators:

- Limit search results to those that match criteria beyond simple keywords.
- Maintain a list of websites, file types, and keywords to search on a regular basis.
- Google allows users to create searches and periodically receive email alerts of new content that matches those searches.

[http://www.googleguide.com/advanced\\_operators\\_reference.htm](http://www.googleguide.com/advanced_operators_reference.htm)  
<http://www.google.com/alerts>

THOMAS P. DINAPOLI

## Information Disposal and Media Sanitization

**Best Practice:** Adopt written policies and procedures that outline the proper process to use in verifying that personal, private and sensitive data is entirely destroyed or removed from electronic media prior to the equipment's disposal or reuse.

Local governments can contract with third parties who specialize in information disposal and media sanitation. Prior to doing so, the entity can, among other things, review and evaluate the disposal company's information security policies, require that the company be certified by a recognized trade association or similar third party, and/or require the company to provide written certification that information was disposed of in the agreed-upon manner.

National Institute of Standards and Technology <http://www.nist.gov/>

THOMAS P. DINAPOLI

## Contracts for IT Support Services

**Best Practice:** Contracts (service level agreements or SLAs) for IT support services should be in writing, clearly state the local government's security needs and expectations, and specify the level of service to be provided by the independent contractor or vendor.

The components of an SLA vary but can include: identification of the parties to the contract; definitions of terminology; term/duration of agreement; scope/subject; limitations (what, if anything, is excluded); service level objectives and performance indicators; roles and responsibilities; nonperformance impact; pricing, billing and terms of payment; security procedures; audit procedures; reporting; reviews/updates; and approvals.

THOMAS P. DINAPOLI

## Contracts for IT Services



For your protection and to avoid potential misunderstandings, there should be a written agreement with your IT service provider.

The written agreement should include:

- *Term/duration of the agreement*
- *Detailed description of the nature and scope of the services provided, including any limitations*
- *Service level objectives and performance indicators.*

The written agreement between the local government and the IT service provider should also state:

- *Roles and responsibilities of the parties*
- *Security procedures, especially relating to protection of data*
- *Costs, billing procedures, and terms of payment*
- *Procedures for reviewing and updating the agreement.*

Establish measurable targets

THOMAS P. DINAPOLI

## Virus Protection



Viruses can corrupt data and make computers and networks inoperable.

**Best Practice:** It is essential that the local government:

- Install and maintain antivirus software applications
- Periodically scan for threats throughout each day
- Update virus definitions daily
- Disable the auto-play feature for mobile storage devices
- Enforce automatic scans of external storage devices.

THOMAS P. DINAPOLI

## Patch Management



- A patch is software created to correct a problem that exists within an application or an operating system.

**Best Practice:** To protect against infection from malware, spyware or other malicious agents due to software vulnerabilities:

- Adopt patch-management policies and procedures that ensure that all patches and updates are applied on a regular basis.
- Apply patches promptly to reduce risk of infection.
- Adopt policies and procedures to ensure that all patches and updates are regularly installed on all computer equipment.

THOMAS P. DINAPOLI

## Access Controls

**Best Practice:** Know all points of entry to your computing environment and data, and ensure that all access is authorized and secure. Use available electronic means to enforce and monitor compliance with access controls. Place particular emphasis on limiting access to and protecting personal, private, and sensitive information.

- Have written procedures in place for granting, changing, and terminating access rights.
- Allow users to access only what is necessary to complete their job duties (principle of least privilege).
- Periodically review all accounts and disable any account that cannot be associated with an authorized user.

BYE COMPLIANCE  
THOMAS P. DINAPOLI

## Access Controls



### Best Practices:

- Written procedures for granting, changing, and terminating access.
- Update rights as necessary (e.g., retirements, terminations).
- Each user should have his or her own network and application accounts and passwords.
- Assign access based on what users need to complete their jobs.
- Users should set their own passwords.
- Hold passwords to complexity requirements to make them more difficult to crack.
- Periodically compare employee master list to list of network and application user accounts.



BYE COMPLIANCE  
THOMAS P. DINAPOLI

## User Accounts and Passwords

- To ensure individual accountability within the network, each user should have his or her own network account (username and password). Likewise, to ensure individual accountability within software applications, each user should have his or her own user account (username and password).
- Criteria you should consider with regard to passwords:
  - Complexity requirements
  - Length
  - Aging
  - Reuse of old passwords
  - Failed log-on attempts.

BYE COMPLIANCE  
THOMAS P. DINAPOLI

## Online Banking



**Best Practice:** Entities should adopt a suite of technology-based and nontechnical controls to ensure online banking is conducted as safely as possible.

- Adopt an online banking policy and enter into bank agreements.
- Segregate duties.
- Enable alerts and other security measures available from the bank.
- Set up accounts that do not have access to and/or cannot be accessed through the Internet, and use those accounts for long-term savings.
- Provide cybersecurity training to officers and employees responsible for online banking.
- Consider using a separate (dedicated) computer for online banking transactions, one that is not used for email or Internet browsing.

BYE COMPLIANCE  
THOMAS P. DINAPOLI

## Online Banking



- The ease and speed with which large amounts of money can be transferred requires that attention be paid to technical and non-technical internal controls over online banking.
- Non-technical controls:
  - Proper segregation of duties.
  - Timely reviews of online banking transactions.
  - Any suspicious activity should be immediately reported to banking officials and/or law enforcement.
- Key technical control:
  - Whenever possible, a wired rather than a wireless network should be used for financial transactions.

BYE COMPLIANCE  
THOMAS P. DINAPOLI

## Online Banking

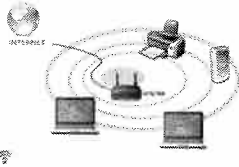
(Continued)

- Type the bank's website address into the Internet browser's address bar every time.
- Do not allow the computer or web browser to save online banking login names or passwords.
- Use a wired rather than wireless network for financial transactions.
- Monitor accounts on a timely basis, at least every two or three days, for unauthorized or suspicious activity.
  - Any suspicious activity should be reported immediately. There is a limited recovery window, and a rapid response may prevent additional losses.
  - To be effective, monitoring must occur frequently even during times when many personnel may be on leave (e.g., 4<sup>th</sup> of July week; the weeks before, during and immediately after Christmas).

BYE COMPLIANCE  
THOMAS P. DINAPOLI

## Wireless Networks

- Wireless networks are exposed to many of the same types of threats as wired networks.
- Wireless networks are considered inherently less secure than wired networks because their information-bearing signals are broadcast or transmitted into the air.
  - Traveling signals can, potentially, be intercepted and exploited by individuals with malicious intent.



WITH CONSULTING BY  
THOMAS P. DINAPOLI

## Wireless Networks

**Best Practice:** Configure your wireless network to broadcast only as far as necessary, enable the best available encryption, and require strong passwords.

- Wireless access point coverage should radiate out to the windows, but not beyond.
- Enable the **most-secure encryption** available (currently WPA2).
- Require a **strong password** for connecting to the wireless network.

WITH CONSULTING BY  
THOMAS P. DINAPOLI

## Firewalls & Intrusion Detection



**Firewalls:** Analyze network traffic and allow or block it based on existing policies.

- Monitor logs for suspicious activities.

**Best Practice:** Install one or more securely configured firewalls, and monitor the logs and alerts the firewall(s) generate. Update the firewall rules as necessary using a formal change management control process.

**Intrusion Detection Systems (IDS):** Analyze traffic in various parts of a network.

- Use IDS to selectively identify attempted unauthorized logical and physical access.
- Routinely review identified activities and investigate possible violations.

WITH CONSULTING BY  
THOMAS P. DINAPOLI

## Physical and Environmental Security

**Best Practices:** Periodically assess physical and environmental security measures to ensure they adequately protect computer resources and the facilities or infrastructure that house or support those resources from intentional or unintentional harm, loss or impairment.

- Physical access controls restrict the entry and exit of personnel and/or equipment and media from an area.
- Locks, gates and security personnel.
- Smoke detectors, fire alarms and extinguishers, protection from water damage due to plumbing leaks or other flooding, and uninterruptible power supplies.



WITH CONSULTING BY  
THOMAS P. DINAPOLI

## Physical and Environmental Security

(Continued)

An organization's personnel can play an important part in physical security by being trained and encouraged to question people whom they do not recognize in restricted areas.

It is important to consider and evaluate physical security measures both during normal business hours and at other times for example, when an area or building may be unoccupied.

**DO YOU KNOW WHERE YOUR SERVERS ARE LOCATED?**

We have found servers:

- On a basement floor in a municipality that experienced flooding in the past.
- Next to the refrigerator in a break room.
- In an open area in a recreation center.
- In a closet used daily by staff and visitors to the facility.

WITH CONSULTING BY  
THOMAS P. DINAPOLI

## IT Disaster Recovery Planning

**Best Practice:** Develop a formal IT disaster recovery plan that addresses the range of threats to your IT system(s), distribute the plan to all responsible parties, and ensure that it is periodically tested and updated as needed.

- The plan should focus on sustaining critical business functions during and after a disruption.
- Technology recovery strategies should consider the possible restoration of hardware, applications, data and connectivity.
- The plan should include policies and procedures to ensure that all critical information is routinely backed up so that it would be available in the event of an emergency.



WITH CONSULTING BY  
THOMAS P. DINAPOLI

## Backups



**Best Practice:** Back up data at regular intervals; verify the data has been backed up; store the backup media in a secure, off-site location; and verify the ability to restore the data backup.

While many entities perform some type of backup procedures, far fewer periodically attempt to restore a backup to ensure the process is functioning as intended and that data would be available in the event of an emergency.

As noted in the following discussion of ransomware, it is important to maintain offline copies of backups in case an attack renders online files unusable.

THOMAS P. DINAPOLI

## Growing Cybersecurity Threat: RANSOMWARE



THOMAS P. DINAPOLI

## Ransomware Scenario

**Imagine the following:** You are locked out of your computer, your computer has been infected with malware, or your data has been deleted or stolen and someone contacts you demanding that you pay a fee or fine (ransom) to regain access to your computer system and data.

What actions should you take?

THOMAS P. DINAPOLI

## Ransomware

Criminals create links and websites that install malware (ransomware) on the computers of unsuspecting computer users and then display messages demanding payment in exchange for restoring the computer to its previous functioning state.

The message may even falsely claim to originate from a law enforcement agency and demand that you pay a "fine" (ransom) to avoid prosecution for illegal activity (e.g., using unauthorized software, downloading illegal content from the Internet) detected on your computer and regain access to your system or files.

THOMAS P. DINAPOLI

## Ransomware Recommendation #1: Do Not Pay the Ransom Before Contacting Cybersecurity Experts

There is no guarantee that paying a ransom will ensure the availability of the computer system and data, protect the computing environment and resources, or prevent future ransom demands.

Cybersecurity experts can assist in determining the best way to proceed and may be able to lend free technical expertise necessary to investigate and remedy or resolve the problem.

THOMAS P. DINAPOLI

## Cybersecurity Experts

Center for Internet Security's Multi-State Information Sharing & Analysis Center

<http://msisac.cisecurity.org/about/>

New York State Office of Information Technology Services

<http://www.its.ny.gov/incident-reporting>

Industrial Control Systems Cyber Emergency Response Team

<https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team>

THOMAS P. DINAPOLI



## Ransomware Recommendation #2: Consult with Your Legal Counsel

Individuals and organizations that demand ransoms for the safe restoration of the functionality of computer systems are breaking the law. Their attempts to "extort" money should be discussed with your legal counsel, who can assist with reporting the incident to law enforcement.

Depending on the nature of the incident, you may have notification requirements under the New York State Breach Notification Law. Legal counsel can assist you in determining if the incident has triggered notification requirements and in complying with those notifications, as necessary.

WITH COMPLIANCE  
THOMAS P. DINAPOLI

## Ransomware Recommendation #3: Consult with Your Insurance Provider

Depending on the nature of the incident and the type of insurance coverage your organization has, you should consider contacting your insurance provider to report the incident.

WITH COMPLIANCE  
THOMAS P. DINAPOLI

## Ransomware: Paying the Price

A local government or school district may ultimately have to pay money to regain access to its computer system and data, but we recommend doing so only after obtaining technical assistance and advice from experts.

WITH COMPLIANCE  
THOMAS P. DINAPOLI

## Ransomware Defense #1: Provide Employees With Cybersecurity Training Before A Problem Occurs

Training can help computer users to: understand their employer's computer policies and their personal responsibilities with respect to those policies; adopt safe computing practices; and know how to react in the event of a suspected problem.

The time to provide cybersecurity training is *before* a problem such as a ransom demand occurs.

WITH COMPLIANCE  
THOMAS P. DINAPOLI

## Ransomware Defense #2: Perform Backups in A Timely Manner And Maintain Copies Offline And Offsite

On a test basis, periodically restore backups to ensure they will function as intended in the event of an emergency.

Good backup procedures minimize potential business disruptions and lessen an attacker's leverage.

WITH COMPLIANCE  
THOMAS P. DINAPOLI

## Ransomware Defense #3: Apply Software Patches And Updates In A Timely Manner

A "patch" is software that is used to correct a problem, such as a security vulnerability, that exists within an application or an operating system. Security vulnerabilities in software can be exploited to infect a computer with malware.

When security vulnerabilities in software are discovered, the software vendor typically issues a free patch (fix) to correct the problem.

WITH COMPLIANCE  
THOMAS P. DINAPOLI

### Ransomware Defense #4: Install And Keep Antivirus Protection Up-To-Date

Antivirus software is used to prevent, detect and remove computer viruses that can make computers and computer networks inoperable.

Antivirus protection should be installed and configured to run periodic, full system scans, as well as to update the virus definitions daily.

NY STATE COMPTROLLER  
THOMAS P. DINAPOLI

### Ransomware Defense #5: Control Administrative Privileges

When malware infects a computer, it is installed and operates under the permissions of the current user – the person who opened the email attachment or visited the infected website.

Ensuring that general-purpose users are not given administrative-level privileges will help to reduce the impact of a malware infection by limiting its capabilities on the infected computer.

NY STATE COMPTROLLER  
THOMAS P. DINAPOLI

### Ransomware Defense #6: Implement Application Whitelisting

An application whitelist is a list of applications that an entity decides are authorized to be present or active on its computer system.

The goal of the technology used to enforce an application whitelist is to stop the execution of unauthorized software including malware.

Application whitelisting is more practical to implement in computer environments that are centrally-managed and where the entity has sufficient, knowledgeable personnel to devote to implementing and maintaining the control.

NY STATE COMPTROLLER  
THOMAS P. DINAPOLI

### Ransomware: Detective Capability of Logs

An audit log is a computer-generated series of records about computer events pertaining to operating systems, applications and computer-user activities. A computer system often has several types of audit logs, each devoted to a specific type of activity.

Enabling and reviewing logs can provide information about previous or current attacks against the organization, as well as assist with any response activities following the discovery of an incident or compromise.

NY STATE COMPTROLLER  
THOMAS P. DINAPOLI

### Resources from OSC

- Training (recorded and live)
- Audit Reports
- Technical Assistance
- Local Government Management Guides:
  - Industrial Control Systems Cybersecurity
  - Information Technology Contingency Planning
  - Information Technology Governance
  - Ransomware
  - Wireless Technology and Security

<http://www.osc.state.ny.us/localgov/index.htm>

NY STATE COMPTROLLER  
THOMAS P. DINAPOLI

### Contact Information

Karen Bryerton  
Office of the State Comptroller  
Division of Local Government & School Accountability  
Associate Examiner Applied Technology  
[kbryerton@osc.state.ny.us](mailto:kbryerton@osc.state.ny.us)  
(315) 428-3206

NY STATE COMPTROLLER  
THOMAS P. DINAPOLI

Thank You



**Division of Local Government and School Accountability**  
[localtraining@osc.state.ny.us](mailto:localtraining@osc.state.ny.us)

  
NEW YORK STATE  
THOMAS P. DI NAPOLI