Cybersecurity for Local Governments and Schools

A Weekly Cybersecurity Awareness Month Web Series

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Week 1 – WHERE Do We Start???

Zachary Maio, Municipal Auditor
Jessica Prevost-Allen, Municipal Auditor
Division of Local Government and School Accountability

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Categories

- **Personal, Private and Sensitive Information (PPSI)**
- **IT Asset Inventories**
- **Policies and Procedures**
- **IT Security Awareness**
- **Written IT Agreements**
- Website Content
- Internet Use
- Malicious Software
- User Accounts and Permissions
- Passwords
- Networks and Computers
- Wireless Access
- Physical Access
- Disaster Recovery
- Audit Trails and Logs

Personal, Private and Sensitive Information (PPSI)

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Personal, Private and Sensitive Information

- Threat
  - Unauthorized disclosure of personal, private or sensitive information
- Attack
  - Leakware: City of Torrance, California (March 2020)
- Best practice
  - Classify data in categories (e.g., public, internal use, confidential) that will help determine the appropriate levels of internal controls needed.

What is PPSI?

Personal, Private and Sensitive Information: Any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact the organization, its critical functions, its employees, its customers, third parties, or citizens of New York.

What is an Individual's PPSI?

- Social Security Number
- Drivers License Information
- Identification Card Number
- Financial Account Information
- Credit Card Information
- Security Codes, Passwords, PINs, Biometric Data
- Mother's maiden name
- Health Insurance Information
- Policy Number
- Health Information

Other Types of PPSI

- Specific structural, operational, or technical information:
  - Mechanical or architectural drawings;
  - Floor plans;
  - Operational plans or procedures;
  - Other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure;
  - Security procedures at sensitive facilities and locations; and
  - Plans for disaster recovery and business continuity.
- Contract information
- Other information that is protected from disclosure by law or relates to subjects and areas of concern as determined by executive management.

What to do with PPSI

- If you don't need it, don't collect it.
- If you collected it, but don't need it, don't keep it.
  - Remove it from your system safely and completely.
- If you collected it and need it:
  - Inventory it; and
  - Protect it.

Protecting PPSI

- Safe Storage
  - Encrypt
    - ALL devices
    - Especially on walkable devices
- Restrict Access
  - Who can access what
- Restrict Permissions
  - What they can do with the data (read, write, modify, delete, move)
- Training Employees
  - Safe Use
    - Do's and Don'ts
  - Safe Transmission

NYS COMPTROLLER THOMAS P. DiNAPOLI 10

IT Asset Inventories

NYS COMPTROLLER THOMAS P. DiNAPOLI

IT Asset Inventories

- Threat
  - IT asset theft or loss
- Attack
  - 37 stolen laptops: Ventura High School, California (March 2020)
- Best practice
  - Maintain inventory records of all computer hardware, software and electronic data to help ensure these IT assets remain protected.

NYS COMPTROLLER THOMAS P. DiNAPOLI 12

What Needs to be Inventoried?

- Hardware Assets
  - Computers
  - Networking Equipment
  - Mobile Devices
- Software
  - Operating Systems
  - Third Party Software
- PPSI
  - Type
  - Location

Inventory Should Include

Hardware

- Serial number
- MAC address
- Unit Name/Type
- Condition
- Location (Physical/Logical)
- Person in possession of equipment (if relevant)
- Static IP address (if relevant)

Software

- Software Version
- Number of Licenses available/used
- Vendor Name
- Hardware it is installed on
- End of support date
- Software Use

Why Keep a Hardware Inventory?

Hardware

- Identify theft and missing equipment
  - South Carolina's Greenville County school district missing Chromebooks ($1.2M)
  - California's Ventura High School stolen Laptops
- Trusted and Approved hardware
  - Malicious hardware planting
- Legacy Equipment
- Vulnerable Hardware/Firmware Patching

Why Keep a Software Inventory?

Software

- Approved Software
  - Identify unapproved installed software
  - Verify licensing compliance
- Version Consistency
  - Verifying software version unification
  - An updated inventory can assist in the automation of this
- Software Updating and Patching
  - Keeping software up-to-date
  - Monitor the support cycle of software

NYS COMPTROLLER THOMAS P. DiNAPOLI 16

Keeping an Inventory of PPSI

You want to know what **TYPE** of PPSI it is and **WHERE** it is Stored.

- Type:
  - Is it an individual's data? (Customer/Employee)
    - Personal or Identifiable
    - PCI-DSS Protected
    - HIPAA Protected
  - Is it business critical or confidential?
- Storage:
  - Logically
    - Where is it stored in the computer system?
  - Physically
    - What hardware(s) is it stored on?

NYS COMPTROLLER THOMAS P. DiNAPOLI 17

IT Policies and Procedures

NYS COMPTROLLER THOMAS P. DiNAPOLI

Policies and Procedures

- Threat
  - Unsecured personal, private or sensitive information
- Attack
  - Student Charged in Cyberattacks at Miami-Dade Schools (September 2020)
- Best practice
  - Adopt policies to address key IT issues including breach notification, data security and privacy, acceptable use and online banking.

Why are Policies Necessary?

- Policies define appropriate user behavior, establish responsibility and accountability, describe tools and procedures needed to protect data and information systems, and explain the consequences of policy violations.
- Lack of policies and procedures increase the risk that data (including PPSI), hardware and software systems may be lost or damaged by inappropriate access or use.

Required Policies

- Breach Notification
  - Section 208 (8) of the State Technology Law requires municipalities and other local agencies to have adopted a breach notification policy or local law
- Data Security and Privacy
  - Section 2-d Part 121.5(b) of the State Education Law requires each educational agency to adopt and publish a data security and privacy policy

Recommended Policies

- Online Banking
- Acceptable Internet, Email, and Computer Use
- Other key topics to cover in policies
  - Password Security
  - Mobile Devices
  - Wireless Security

IT Security Awareness

NYS COMPTROLLER
THOMAS P. DiNAPOLI

IT Security Awareness

- Threat
  - Inadvertent exposure to network or computer compromise
- Attack
  - Unauthorized download: State of Louisiana (November 2019)
- Best practice
  - Ensure all IT users receive on-going training on emerging IT security threats and trends.

Why is IT Security Awareness Training Needed?

- While the IT policies tell computer users what to do, cybersecurity training provides them with the skills to do it.
  - IT security awareness training should explain the proper rules of behavior for using your IT systems and data, and communicate the policies and procedures that need to be followed.
- Failure to provide IT security awareness training increases the risk that users will not understand their responsibilities, putting the data and computer resources at risk for unauthorized access, misuse or abuse.

Possible Training Topics to Consider:

- Disaster Recovery Procedures
- Physical Security, Clean Desk, Environmental Controls
- Mobile/Removable Devices
- Bring-Your-Own-Device (BYOD)
- Data Classification (PPSI)
- Acceptable Use Policy Requirements
- Social Networking Dangers
- Malware
- Email Scams (phishing)

Training does not have to be elaborate or expensive!

Training Material References

- Center for Internet Security
  - **https://www.cisecurity.org/**
- New York State Office of Information Technology Services
  - **https://its.ny.gov/**
- New York State Office of the State Comptroller
  - **https://www.osc.state.ny.us/**
- United States Department of Education
  - **https://www.schoolsafety.gov/**

Written IT Agreements

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Written IT Agreements

- Threat
  - Gaps and misunderstandings about critical IT security tasks
- Attack
  - Payment card theft: Village of Wellington, Florida and other Click2Gov customers (2017-2018)
- Best practice
  - Establish written agreements with IT service providers that clearly define the services to be provided by the vendor, including any specific needs and expectations that must be met.

What is a Service Level Agreement?

- Establishes specific measureable performance targets
  - Examples:
    - Patch management provided daily, weekly or as updates are released
    - Cloud service provider guarantees access to application a percentage of time and reduces fee if unable to meet target

Why is an IT Services Agreement Needed?

- Increasing reliance on third party IT-related services
- Protection and avoid misunderstandings
  - Responsibilities of vendor are clearly defined so IT operations function as intended and IT assets are protected

What should be included in the agreement?

- Specific level of service to be provided by vendor
- Needs and expectations
- Confidentiality
- Protection of data and information
  - Subcontractors
- Length of agreement

State Education Law Section 2-D

State Education Law requires educational agencies to include the following in any contract that involves sharing student, teacher or principal personally identifiable information (shared PII) with the third-party contractor:

- A requirement to maintain the confidentiality of shared PII.
- A bill of rights supplement.
- The contractor's data security and privacy plan.

Sneak Peek - Week 2

- Website content
- Internet use
- Malicious software
- User accounts and permissions
- Passwords

NYS COMPTROLLER THOMAS P. DiNAPOLI 34

Thank You

Division of Local Government and School Accountability
LGSAAppliedTech@osc.ny.gov

NYS COMPTROLLER THOMAS P. DiNAPOLI 35