Cybersecurity for Local Governments and Schools

A Weekly Cybersecurity Awareness Month Web Series

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Week 2 – IT Contingency Planning

Mandy Hopkins, IT Specialist
Division of Local Government and School Accountability

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Agenda

- Review of IT Governance
- What is IT Contingency Planning?
- Unplanned IT Disruptions
- IT Contingency Planning Best Practices
- Preventive Controls That Could Be Included as Part of an IT Contingency Plan
- Business Continuity Plans and Disaster Recovery Plans
- Backup Procedures
- Backup Procedure Best Practices
- Resources
- Sneak Peek – Week 3

NYS COMPTROLLER
THOMAS P. DiNAPOLI
3

Recap – Week 1

IT Governance

- IT Policy
- IT Security Training and Awareness
- Computer Hardware, Software and Data Inventories
- Contracts for IT Services
- Virus Protection
- Patch Management
- Access Controls
- Online Banking
- Wireless Network
- Firewalls and Intrusion Detection
- Physical Controls
- Information Technology Contingency Planning

What is IT Contingency Planning?

An actionable and defined list of plans, policies, procedures and technical measures used if an unplanned event occurs.

Unplanned IT Disruptions

- Major Natural Disaster
- Human Error
- Malware
- Hardware Failure

IT Contingency Planning Best Practices

Proactively anticipate and plan for IT disruptions by:

- Assembling a team
- Identifying critical processes and services
- Developing a written plan
- Training personnel and testing the plan
- Periodically reviewing and revising the plan

Preventive Controls That Could Be Included as Part of an IT Contingency Plan

- Uninterruptable power supplies (UPS)
- Generators to provide long-term backup power
- Fire suppression systems and fire/smoke detectors
- Plastic tarps to be unrolled over IT equipment to protect it from water
- Heat-resistant/waterproof containers for backup media
- Least-privilege access controls

Business Continuity Plans and Disaster Recovery Plans

Business Continuity Plan (BCP) focuses on keeping organizations operational **during** an unplanned event to limit the downtime (ensuring business survival and ability to remain operational during unusual/unfavorable situations).

Disaster Recovery Plan (DRP) focuses on restoring data access and IT infrastructure **after** an unplanned event, in an effort to reduce overall risk such as data or infrastructure loss (returning operations to normal as quickly as possible).

Backup Procedures

- The **backup** is a copy of electronic information that's maintained for use if there's loss or damage to the original.
- The **backup plan** is the written procedures to put a backup in place.

NYS COMPTROLLER THOMAS P. DiNAPOLI 10

Backup Procedure Best Practices

- Develop a data backup policy.
- Back up at regular intervals.
- Verify data is backed up and can be restored.
- Store backups offsite and offline in a secure, environmentally-controlled location and consider the following:
  - Geography of the facility
  - Accessibility for data retrieval
  - Security capabilities
  - Environment (preventative controls)
  - Costs associated

NYS COMPTROLLER THOMAS P. DiNAPOLI 11

Resources

Office of the State Comptroller
https://www.osc.state.ny.us/files/local-government/publications/pdf/itcontingencyplanning.pdf

Multi-State Information Sharing & Analysis Center (MS-ISAC)
https://cisecurity.org/ms-isac/

National Institute of Standards and Technology (NIST)
https://nist.gov

New York State Office of Information Technology Services (NYS ITS)
https://its.ny.gov

Cybersecurity and Infrastructure Security Agency (CISA)
https://www.cisa.gov

NYS COMPTROLLER THOMAS P. DiNAPOLI 12

Sneak Peek – Week 3

Wireless Technology and Security

- Wireless Technology and Security
- Basic Wireless Technology Concepts
- Best Practices for Wireless

NYS COMPTROLLER THOMAS P. DiNAPOLI 13

Thank You

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

NYS COMPTROLLER THOMAS P. DiNAPOLI 14