Office of the NEW YORK STATE

COMPTROLLER

Protecting Sensitive Data and Other Local Government Assets:

A Non-Technical Cybersecurity Guide for Local Leaders

NYS Comptroller

THOMAS P. DiNAPOLI

JUNE 2016

Introduction

As the chief executive officer of a local government or school district, you have a responsibility to protect and maintain a secure information technology (IT) system.[1] Unfortunately, cybersecurity incidents are common in both public and private sectors.[2] The Office of the New York State Comptroller (OSC) provides many resources to assist you in addressing these risks.

Theft, fraud and inappropriate access to information are among the hazards associated with IT systems. A municipality may face a financial loss or a system failure as a result of cyber-threats. A data breach of personal, private and sensitive information to unauthorized individuals may not only disrupt operations; it can also erode the confidence of the public and of employees who rely on a government's IT network to be safe and secure.

The need for security isn't merely hypothetical: a recent audit of the Village of Ilion described how criminals launched not just one, but two ransomware attacks on the Village, encrypting important and sensitive data and refusing to remove the encryption unless payments were made to the attackers. This cost the Village $800, hours of staff time, and much public embarrassment.[3]

It is not only external threats that you must guard against. OSC conducts regular audits of internal controls for local governments, such as ensuring segregation of duties so that not all disbursement functions are being performed by the same accounts payable clerk. Most local officials recognize that these are an essential part of preventing fraud, yet IT internal controls are often overlooked. Audits conducted by OSC have shown that some types of weaknesses are persistently prevalent in local government and school district IT systems, regardless of the complexity or size of the system. As a local leader, you can take steps now – many of them low cost or no cost – to prevent or mitigate big problems later.[4]

Audits conducted by OSC have shown that some types of weaknesses are persistently prevalent in local government and school district IT systems, regardless of the complexity or size of the system.

Preventing a Cybersecurity Breach

Although no cybersecurity plan will make your IT system bullet proof, there are some best practices that can significantly reduce the odds of a breach. They can also make it possible to recover from cybersecurity incidents in a quicker time frame. Depending on the structure of your local government, one or more people or departments should be involved in these critical steps:

- Performing cybersecurity self-assessments.
- Adopting written IT policies and procedures.
- Providing IT training programs to staff.
- Reviewing and monitoring IT systems on a continual basis.
- Being prepared to recover quickly in the event a breach happens.

Perform a Cybersecurity Self-Assessment

Regularly conducted self-assessments help you identify the IT systems and information that you are responsible for protecting. Any assessment should include key areas of IT internal controls such as policy, training, access and monitoring. It should also identify any risks to data and existing hardware and software. This will allow you to develop a plan to find the solutions that meet your unique IT needs.

A cybersecurity assessment should:

- Determine what personal, private and sensitive information your government collects, and where it resides on your electronic equipment.
- Determine what type of computer hardware and software your organization is currently using. Verify that anti-virus protection as well as software and operating system patches are up-to-date.
- Identify who has access to information within your organization. Insufficient controls over access is one of the areas where audits have found the most persistent problems.
- Review any existing written IT policies and procedures. Determine if you have policies covering data breach notification, disaster recovery, IT service continuity, remote access, employee departure and an acceptable use policy. Find out if employees are aware of and complying with existing policies, as well as when they last had any IT training relevant to their positions.

Based on the assessment, identify appropriate solutions to the weaknesses you have identified. Solutions can range from simple to complex, depending on your needs.[5]

Adopt Written IT Policies and Procedures

You should adopt policies to protect your local government and the people it serves from cybersecurity threats. Some policies are required by law, others are strongly recommended; OSC audits look for both types. In addition, your IT staff should have procedures in place to implement those policies. Written policy documents should be distributed to everyone who accesses your IT system to ensure that they are universally recognized and understood. The documents should be updated periodically, to ensure that they cover all existing technologies and threats. You should identify a specific individual or individuals who will be principally responsible for IT security, including ensuring that proper policies and procedures are in place and being followed.

Policies should cover:

- Data breach notification. Affected parties must be notified if unauthorized individuals obtain sensitive and personal data.[6] A written policy ensures that your employees understand this legal obligation and are prepared to fulfill it.

- IT service continuity and disaster recovery plan. Such a plan enables the recovery of IT operations after an unexpected disruption. *In recent audits, town and villages were more likely than school districts to have poor or nonexistent disaster recovery plans and procedures. These audits found that many municipalities did not back up their data in a secure offline, offsite location, or periodically restore back-up data on a test basis to ensure that the plan would function as intended in case it had to be put into use.*

- Access controls. Controlling access to IT systems and associated information is one of the most important areas for both policies and procedures. Proper implementation of these can reduce risk substantially, yet many local governments have been found on audit not to implement them consistently. Policies and procedures should address the following issues related to IT access:

    - Allowing only authorized individuals to access networks remotely through a remote access policy, in order to provide a safeguard for the network. *Audits conducted by OSC found that local governments and school districts often failed to establish these remote access policies and procedures.*

    - Granting all users access only to those IT resources that are necessary to fulfill their job responsibilities. *Recent OSC audits have found instances where employees had unnecessarily broad access rights to municipal financial systems, or where student account users could access personal, private and sensitive information, including Social Security numbers and bank account information.*

    - Implementing an acceptable-use policy that limits the use of government-issued computers and networks to work-related purposes.

- Establishing unique user logins (User ID) and passwords for each computer user, and for websites and wireless networks. *A recent OSC audit identified a municipality that had an open, unsecured wireless access router, with the default (factory-supplied) name and setting connected to the municipality's server. This deficiency could allow an unauthorized person to access the municipality's computer network, and gain access to sensitive information*. It is important that passwords fulfill minimum standards:
    - Combination of alpha and numeric characters
    - Not based on words easily associated with the user
    - Not stored in a public place
    - Regularly changed.
- "Locking" computers when they are unattended by enabling a computer to lock automatically after a specific time of inactivity and establishing a policy for employees to manually lock them when they leave their work stations.
- Maintaining proper physical controls over IT property:
    - Establish a policy covering the appropriate storage of laptops or other portable IT equipment. For example, employees should not leave laptops visible in parked vehicles.
    - Ensure that employees are granted physical access to IT systems only to accomplish their job responsibilities.
    - Keep computers, servers, removable media (such as USB drives) and other IT system components in a locked and secured area.

- An employee departure checklist. A checklist should be used when an employee leaves the municipality, to ensure that the employee's access to IT accounts is terminated and that any IT equipment within the employee's possession is immediately returned to the local government. A different checklist should be used for employees that change departments or job functions within the municipality, to ensure that access controls and equipment are appropriate for the new function.

Provide IT Training Programs

- Provide regular cybersecurity training for everyone (including employees, officials, interns and contractors) who interacts with a local government's IT system, so that IT policies are reinforced and followed.

- Use free training and resources as needed:

    - The Academy for New York State's Local Officials, Office of the State Comptroller: **www.osc.state.ny.us/localgov/academy/index.htm**

    - The New York State Office of Information Technology Services, Enterprise Information Security Office (EISO): **www.its.ny.gov/awarenesstrainingevents**

    - The Multi-State Information Sharing and Analysis Center: **msisac.cisecurity.org**.

Review and Monitor IT Systems on a Continual Basis

Cyber-criminals are continuously producing new threats to local governments, with some of the newest trends including:

- Industrial control systems (ICS): Traditionally, ICS were not connected to the outside world. However, with advances in technology, there has been a shift to more widely-available, lower-cost IT processes that support Internet connectivity for these systems. This increased connectivity enables ICS operators and other support personnel to monitor the ICS remotely. This also increases the possibility of a potential attack, as evidenced by a reported cyber-attack on a dam near the Village of Rye Brook by operatives linked to the Iranian government. The U.S. Department of Homeland Security has received and responded to 295 ICS cyber-attacks during the fiscal year ending September 30, 2015.[7]

- Ransomware: This type of malware attack has already affected local governments in the State and poses a continuing, and expensive, threat. In the first three months of 2016 alone, the FBI has stated that cyber-criminals have collected $209 million in ransom demands nationwide, and ransomware is on a pace to be a $1 billion crime threat this year.[8] In addition to the Village of Ilion, mentioned above, an employee of the Town of Manlius recently noticed that a ransomware attack was in progress on a Town computer. Fortunately, the Town's IT staff was able to stop the attack before any data was taken and a ransom was demanded. The Town credits the training it provided employees on procedures to follow if they suspect an IT attack, as well as its purchase of cybersecurity insurance, as reasons why the attack ultimately proved unsuccessful.[9]

- Overseas Attacks: Senator Charles Schumer has recently noted that cyber-attacks on upstate New York local governments are becoming more frequent, and many are coming from organized groups in Eastern Europe, making them difficult or impossible to track down.[10] The recent Town of Manlius ransomware attack, for example, was traced to Russian cyber-criminals operating out of Crimea. The FBI requests any local government or individual that falls victim to a ransomware attack or other type of cyber-crime to file a complaint with their Internet Crime Complaint Center (IC3), either through their local FBI field office or through their website, as provided in the Additional Resources section below.

Be aware of the changing world of cybersecurity and make sure you're prepared to deal with the latest trends that can put your community at risk. Key allies in this process will be your own employees, and your most effective strategy will seek to maximize the power of clear communication within the organization.

- Review your written policies, procedures and training frequently, to ensure that these areas are still relevant to the ever-changing IT systems being adopted.

- Update your local government's inventory of IT hardware and software components.

- Regularly check for new updates to your computer's firewall, security software patches and virus protection software.

- Continuously monitor and review IT systems for unauthorized or unusual activity. *OSC audits have found instances where access controls were not monitored, or where user reports were generated but their output was not reviewed. In one instance, even though a municipality could generate an audit log that identified who has accessed their financial software system, this log was never examined*.

Be Prepared for a Cybersecurity Breach

You can greatly reduce your local government's risk of falling victim to cybersecurity attacks by following the steps mentioned above. However, if an attack or breach does occur, there are certain steps an organization should follow:

- Refer to your established data breach notification policy and IT service continuity and disaster recovery plan.
- Contact cybersecurity experts, legal counsel, and insurance providers (depending on the nature of the breach and the type of insurance coverage you have).
- Access additional resources, located in the Appendix section, below. Specifically, OSC has produced the following Local Government Management Guides on IT issues:
    - *Information Technology Governance*, available at **www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf**
    - *Industrial Control Systems Cybersecurity*, available at **www.osc.state.ny.us/localgov/pubs/lgmg/industrialcontrolsystems.pdf**; and
    - *Ransomware*, available at **www.osc.state.ny.us/localgov/pubs/lgmg/ransomware.pdf**.
- Create a log of IT incidents and what actions you have taken. This can be a useful reference to see if any patterns are arising, and provides for a review of actions taken if similar incidents were to arise.[11]

Glossary of Terms

Access Controls: The process of granting or denying specific requests for or attempts to:
1) obtain and use information and related information-processing services; and
2) enter specific physical facilities.

Firewall: Security system that uses hardware and/or software mechanisms to prevent unauthorized users from accessing an organization's internal computer network.

Industrial Control System (ICS): A generic term used to describe any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve a desired result, such as water and wastewater systems.

Information Technology (IT) System: Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives or interchanges data or information.

Malware: A term that is short for "malicious software," malware refers to software programs that are specifically designed to harm computer systems and electronic data. Malware often causes this harm by deleting files, gathering sensitive information and making systems inoperable. Computer users can inadvertently install malware on their computers in many ways, including opening email attachments, downloading free software from the Internet, or merely visiting infected websites.

Ransomware: A unique type of malware that prevents access to a user's computer or electronic data. Criminals create links and websites that install ransomware on the computers of unsuspecting users and then display messages demanding payment in exchange for restoring the computer to its functioning state.

Remote (access): Access to networks from an offsite location.

Router: A hardware device that, if it is wireless, can connect a small number of wired and any number of wireless devices to each other for access to the Internet as well as for file sharing and printing.

Software or Operating System Patches: Fixes to correct a problem. People are constantly finding security holes (i.e., vulnerabilities) in computer software and operating systems, which could be used to infect your computer with a virus, spyware or worse. When vulnerabilities are discovered, the vendor typically issues a fix (i.e., patch) to correct the problem. This fix should be applied as soon as possible, because the average time for someone to exploit the security hole can be as little as a few days.

Unauthorized Access: Any access that violates the stated security policy.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread to another computer.[12]

Additional Resources

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
ics-cert.us-cert.gov

Federal Bureau of Investigations (FBI), Internet Crime Complaint Center (IC3)
(to report a ransomware or other cyber-crime complaint)
www.ic3.gov

Multi-State Information Sharing and Analysis Center (MS-ISAC)
msisac.cisecurity.org

National Institute of Standards and Technology (NIST)—Information Technology Portal
www.nist.gov/information-technology-portal.cfm

New York State Office of Information Technology Services (ITS)
www.its.ny.gov

New York State Office of Information Technology Services,
Enterprise Information Security Office (EISO)
www.its.ny.gov/eiso

Office of the New York State Comptroller (OSC)
www.osc.state.ny.us

United States Department of Homeland Security,
United States Computer Emergency Readiness Team (US-CERT)
www.us-cert.gov

Notes

[1] The "Glossary of Terms" section located in the back of this Guide provides explanations of important IT terms such as "information technology system".

[2] "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," The Washington Post, July 9, 2015, **www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say**;
"Why Hospitals Are the Perfect Targets for Ransomware," Wired, March 30, 2016, **www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets**;
"Target Settles for $39 million Over Data Breach,' CNN Money, December 2, 2015 **money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement**.

[3] For more information on Industrial Control Systems (ICS) and Ransomware, see the OSC Local Government Management Guides on these topics: Industrial Control Systems Cybersecurity, Reprinted January 2016, available at **www.osc.state.ny.us/localgov/pubs/lgmg/industrialcontrolsystems.pdf**;
and Ransomware, October 2015, available at **www.osc.state.ny.us/localgov/pubs/lgmg/ransomware.pdf**.
Also see the OSC audit of the "Village of Ilion: Information Technology," 2015M-34, July 2015.

[4] "Cyber Security: Getting Started, A Non-Technical Guide Essential for Executives and Managers," Multi-State Information Sharing and Analysis Center and NYS Office of Information Technology Services, NYS Enterprise Information Security Office, 2012. To access this guide as well as other cybersecurity guides. See: **www.its.ny.gov/local-government**.

[5] For more information and to see a template of an IT Security Self-Assessment, access the OSC Local Government Management Guide, *Information Technology Governance*, Updated March 2016, available at **www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf**.

[6] Adoption of this policy is a requirement for a local government under State Technology Law Section 208(8).

[7] "Iranian Hackers Infiltrated New York Dam in 2013," *The Wall Street Journal*, December 20, 2015, **www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559**.

[8] "Cyber-Extortion Losses Skyrocket, Says FBI," CNN Money, April 15, 2016, **money.cnn.com/2016/04/15/technology/ransomware-cyber-security**.

[9] "CNY Town's Computer Attacked by 'Ransomware' from Russia; How to Recognize It, Stop It," Syracuse Post-Standard, March 14, 2016, **www.syracuse.com/news/index.ssf/2016/03/ransomware_targets_cny_town_how_to_recognize_and_prevent_it.html**.

[10] "Schumer Reveals: Russian Hackers Zeroing In on Upstate NY; Forcing Small Governments to Pay Big Bills to Remove 'Ransomware' That Can Breach Municipal Computer Systems; Upstate Towns and Villages Are Easy Prey For Hack Attack That Ends Up Costing Local Taxpayers & Could Jeopardize Personal Info; Senator Urges Feds to Give Local Governments The Tools to Fight Back," *Press Release from U.S. Senator Charles E. Schumer*, May 18, 2016, **www.schumer.senate.gov**.

[11] See a sample incident log template at "Cyber Security: Cyber Incident Response Guide, A Non-Technical Guide Essential for Executives and Managers," Multi-State Information Sharing and Analysis Center and NYS Office of Information Technology Services, NYS Enterprise Information Security Office, 2013.

[12] Definitions provided by: "Explore Terms: A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, U.S. Department of Homeland Security, niccs.us-cert.gov/glossary; "Cyber Security: Cyber Incident Response Guide, A Non-Technical Guide Essential for Executives and Managers," Multi-State Information Sharing and Analysis Center and NYS Office of Information Technology Services, NYS Enterprise Information Security Office, 2013; "Cyber Security: Getting Started, A Non-Technical Guide Essential for Executives and Managers," Multi-State Information Sharing and Analysis Center and NYS Office of Information Technology Services, NYS Enterprise Information Security Office, 2012.

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability

110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.state.ny.us

www.osc.state.ny.us/localgov/index.htm

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller