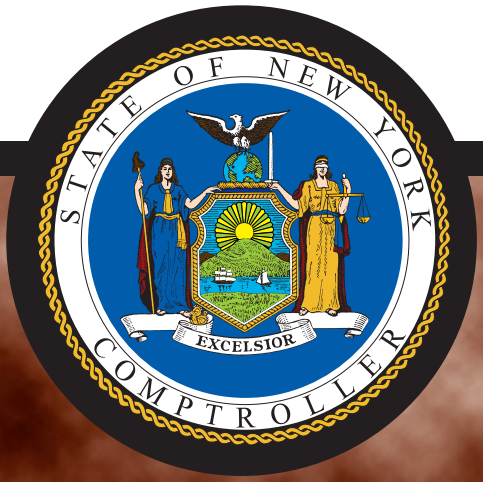
Office of the New York State Comptroller
Thomas P. DiNapoli, State Comptroller
Division of Local Government and School Accountability

LOCAL GOVERNMENT MANAGEMENT GUIDE

Ransomware



For additional copies of this report contact:

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th floor
Albany, New York 12236
Tel: (518) 474- 4037
Fax: (518) 486- 6479
or email us: localgov@osc.state.ny.us

www.osc.state.ny.us

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

October 2015

Table of Contents

Ransomware

Imagine being locked out of your computer because it has been infected with malware, or having data and records deleted or stolen and then being contacted by someone demanding a fee or fine (ransom) to regain access to the computer system and data.

Malicious software, or malware, refers to software programs that are designed to harm computer systems. These programs can wreak havoc on both systems and electronic data by, for example, deleting files, gathering sensitive information such as passwords without the computer user's knowledge and making systems inoperable. Computer users can inadvertently install malware on their computers by many methods, including opening email attachments, downloading content from the Internet or merely visiting infected websites.

Ransomware is 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. The message may even falsely claim to originate from a law enforcement agency and demand that the recipient pay a fine to avoid prosecution for illegal activity (e.g., using unauthorized software, downloading illegal content from the Internet) detected on the computer and regain access to the system or files. A typical ransomware demand may appear in the form shown in the example below:[1]

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.

[1] From the Federal Bureau of Investigations Internet Crime Complaint Center at **http://www.ic3.gov/media/2013/131028.aspx**

Instances of ransomware are increasingly affecting users worldwide and are unlikely to subside anytime soon as they generate a significant amount of revenue for cybercriminals.

Criminals have used ransomware to target home computers, financial institutions, government agencies, academic institutions and other organizations. Instances of ransomware are increasingly affecting users worldwide and are unlikely to subside anytime soon, as they generate a significant amount of revenue for cybercriminals.

New York State Technology Law (State Technology Law) requires municipalities and other local agencies to have a breach notification policy or local law.[2] Such policy or local law must require that notification be given to certain individuals when there is a breach of the security of the system as it relates to private information.

While New York State Information Security Policy requires State government entities to notify the Cyber Incident Response Team (CIRT) of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to ensure proper incident response procedures, coordination and oversight,[3] there currently is no similar type of requirement or mechanism for cyber incidents involving local governments. Such a requirement could help increase awareness of cyber incidents among local governments and standardize responses.

Proper information technology (IT) security and preparation can reduce the risk of local governments becoming a victim of ransomware and data breaches. Appropriate measures include providing IT security training to all employees, implementing and enforcing an acceptable-use policy, maintaining offline backup copies of all critical data, limiting the number of users granted administrative privileges,[4] installing and keeping antivirus protection up-to-date, and applying software patches and updates in a timely manner.

[2] Section 208 (8) of the State Technology Law requires municipalities and other local agencies to have adopted a breach notification policy or local law consistent with the requirements contained in Section 208 by April 6, 2006. Pursuant to Section 208, notification is required to be given to certain individuals when there is a "breach of the security of the system" as it relates to "private information." "Breach of the security of the system" is generally defined as meaning unauthorized acquisition of computer data which compromises the security, confidentiality, or integrity of personal information maintained by the entity. "Private information" is defined as personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

[3] See New York State Office of Information Technology Services at **https://www.its.ny.gov/incident-reporting.**

[4] Administrative privileges allow users to: access all data on a system, including data created and stored by other users; make changes to the settings configured on the system, including disabling antivirus software; and create new user accounts or change the levels of privileges granted to existing user accounts.

Ransom Demands

Before paying a ransom demand:

- Contact cyber security experts, who can help determine the best way to proceed and may be able to lend free technical expertise necessary to investigate and resolve the problem. A few organizations that investigate and provide this guidance include:
  - Center for Internet Security's (CIS) 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**); and
  - Industrial Control Systems Cyber Emergency Response Team (**ICS-CERT) (https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team**).
- Consult insurance providers. Depending on the nature of the incident and the type of insurance coverage the entity has, officials should consider contacting their insurance provider to report the incident.
- Consult legal counsel. Individuals and organizations that demand ransoms for the safe return of the functionality of computer systems are breaking the law. Their attempts to "extort" money should be discussed with the entity's legal counsel who can assist with reporting the incident to law enforcement. In addition, depending on the nature of the incident, there may be breach notification requirements. Legal counsel can assist in determining if the incident has triggered the notification requirements and in complying with those requirements, as necessary.

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

Individuals and organizations that demand ransoms for the safe return of the functionality of computer systems are breaking the law.

Best Practices

Provide employees with cybersecurity training before a problem occurs.

Policies and procedures that can help to reduce the chances of being a victim of ransomware, or help you understand what happened and restore systems if an incident occurs, include the following:

- Ensure that your local government or school district has adopted a disaster recovery plan which includes procedures and information to aid in effectively responding to and recovering from events that impair or potentially impair IT security; test the recovery plan periodically.
- Provide employees with cybersecurity training before a problem occurs.
- Perform backups of applications and data in a timely manner and maintain offline, offsite copies.
- Apply software patches and updates in a timely manner.
- Install and keep antivirus protection up-to-date.
- Control the use of administrative privileges.
- Enable and review audit logs.
- Adopt a breach notification policy or local law consistent with State Technology Law requirements.

Division of Local Government and School Accountability

Central Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

(Area code for the following is 518 unless otherwise specified)

Executive 474-4037
Gabriel F. Deyo, Deputy Comptroller

Audits, Local Government Services and Professional Standards 474-5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line ..... (866) 321-8503 or 408-4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

New York State & Local Retirement System

Retirement Information Services

Inquiries on Employee Benefits and Programs 474-7736

Bureau of Member and Employer Services ..... (866) 805-0990 or 474-1101

Monthly Reporting Inquiries 474-1080

Audits and Plan Changes 474-0167

All Other Employer Inquiries 474-6535

Division of Legal Services

Municipal Law Section 474-5586

Other OSC Offices

Bureau of State Expenditures 486-3017

Bureau of State Contracts 474-4622

Mailing Address for all of the above:

Office of the New York State Comptroller,
110 State Street, Albany, New York 12236
email: **localgov@osc.state.ny.us**

Division of Local Government and School Accountability

Regional Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

Gabriel F. Deyo, Deputy Comptroller (518) 474-4037

Cole H. Hickland, Director • **Jack Dougherty**, Director
Direct Services (518) 474-5480

BINGHAMTON REGIONAL OFFICE - H. Todd Eames, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313 • **Email:** Muni-Binghamton@osc.state.ny.us
Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • **Fax** (716) 847-3643 • **Email:** Muni-Buffalo@osc.state.ny.us
Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

GLENS FALLS REGIONAL OFFICE - Jeffrey P. Leonard, Chief Examiner
One Broad Street Plaza • Glens Falls, New York 12801-4396
Tel (518) 793-0057 • **Fax** (518) 793-5797 • **Email:** Muni-GlensFalls@osc.state.ny.us
Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner
NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533
Tel (631) 952-6534 • **Fax** (631) 952-6530 • **Email:** Muni-Hauppauge@osc.state.ny.us
Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner
33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725
Tel (845) 567-0858 • **Fax** (845) 567-0080 • **Email:** Muni-Newburgh@osc.state.ny.us
Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner
The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608
Tel (585) 454-2460 • **Fax** (585) 454-3545 • **Email:** Muni-Rochester@osc.state.ny.us
Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner
State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428
Tel (315) 428-4192 • **Fax** (315) 426-2119 • **Email:** Muni-Syracuse@osc.state.ny.us
Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

STATEWIDE AUDIT - Ann C. Singer, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313

Office of the New York State Comptroller • Thomas P. DiNapoli, State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor • Albany, New York 12236