

Local Government Information Security: Getting Started

A Non-Technical Guide

***Essential for
Elected Officials
Administrative Officials
Business Managers***



**Multi-State Information
Sharing and Analysis Center
(MS-ISAC)**

Special thanks and appreciation to the members of the NYS Local Government Cyber Security Committee whose dedication and passion to this effort made this Guide possible:

Joyce Bellinghausen, NYS Department of Criminal Justice Services; **Wade Beltramo**, NYS Conference of Mayors; **Greg Benson**, NYS Forum; **Thomas Bodden**, NYS Association of Towns; **Bob Brownell**, NYS Office of the Inspector General; **Meghan Cook**, Center for Technology in Government; **Michael Donovan**, NYS Chief Information Office; **Mark Dorry**, Albany County; **Thomas Duffy**, NYS Office of Cyber Security & Critical Infrastructure Coordination; **Stan France**, Schoharie County; **Steven Geurds**, New York Association of Local Government Records Officers; **Geof Huth**, NYS Archives; **Laura Iwan**, NYS Office of Cyber Security & Critical Infrastructure Coordination; **Alan Kowlowitz**, NYS Office for Technology; **Dave Koschnick**, NYS Office of Real Property Services; **Krista Montie**, NYS Office of Cyber Security & Critical Infrastructure Coordination; **Timothy Oxborough-Powell**, NYS Office for Technology; **James Page**, NYS School Boards Association; **Tina Post**, NYS Office of Cyber Security & Critical Infrastructure Coordination and **Tina Ward Stuart**, Town of Cobleskill, NY.

In addition, the following individuals reviewed the drafts and provided additional comments to help ensure we were meeting the needs of our target audience: **Cathy Herzog**, Town of Ontario, NY; **Helen Kopke**, Town of Niskayuna, NY and **Michelle Schimel**, Town of North Hempstead, NY.

Thanks also to the following MS-ISAC members for reviewing this Guide and making very helpful suggestions: **Darrell Davis** from Alaska, **Eva Doud** from Oregon, **Greg Fay** from Iowa, **Dan Lorchmann** from Michigan, **Chris Turpin** from North Carolina and **Elayne Starkey** from Delaware.

THANK YOU!

The "Local Government Information Security: Getting Started" Guide has been developed and distributed for educational and non-commercial purposes only. Copies and reproductions of this content, in whole or in part, may only be distributed, re-produced or transmitted for educational and non-commercial purposes.

Dear Elected Official, Administrative Official and Business Managers,

Welcome to the "Local Government Information Security: Getting Started Guide," and congratulations on taking an important step in furthering your knowledge and awareness regarding cyber security. This Guide is one of the first primary deliverables of the New York State Local Government Cyber Security Committee.

Because cyber security knows no geographic boundaries, the information contained in this Guide is applicable not only to localities in New York State, but across the nation as well. To that end, we've partnered this effort with the Multi-State Information Sharing and Analysis Center (MS-ISAC), a voluntary organization comprising all 50 states and the District of Columbia, focused on enhancing our cyber posture.

This Guide is geared for a non-technical audience and we recommend distribution to all board members and business managers in your government. It should also be shared with those who implement your information technology as well as with the individual(s) responsible for information security in your government.

Future installments of this Guide will include more in-depth appendices that provide the detailed steps necessary to secure the information which your citizens have entrusted to you.

*We look forward to your comments on this Guide. Please take a few moments to complete and return the survey or click on **Getting Started Survey** at <http://www.cscic.state.ny.us/msisac/index.html>. In return for providing us with your comments we will provide you with a cyber security toolkit with free resources for furthering your cyber security knowledge base.*

*William F. Pelgrin
Director,
NYS Office of Cyber Security and
Critical Infrastructure Coordination and
Chair
MS-ISAC*

Local Government Information Security: Getting Started

This guideline is intended for elected officials, administrative officials of cities/towns/villages and other local government jurisdictions. It is designed to demystify cyber security and to provide a clear, concise and achievable approach to improve local government's cyber security posture.

Information security can seem overwhelming to many. When you hear statistics that some 10,000 new computer viruses were reported last year, it is not hard to imagine the impact a virus or computer compromise can have on our networks and the information contained within those systems. However, if you do not have the knowledge base or resources to address these threats, you may feel helpless. Especially for those with a lack of experience or resources to address the constant evolving and increasing threats from cyberspace, it is difficult to know what to do or how to get started. Often it is the start that stops most of us.

Information security is a basic concept. As local government leaders, you are responsible for protecting the information in your care. Information security is a business function, and technology is a tool that can be used to more securely protect information assets. While addressing information security may seem like a daunting task, it is much more palatable if taken in manageable chunks. Information security runs the gamut from simple physical security steps (making sure your laptops and other portable media are secured when not in use) to implementing large-scale information technology systems (*firewalls*, incident detection and prevention systems, anti-virus and anti-*spyware* software).

Solutions can be low cost and simple to implement, high cost and complex, or somewhere in between. The important point is to identify what you are responsible for protecting and implementing a mix of solutions that best meets your business needs. The good news is there are many resources available to help you establish an efficient and effective information security program. This guide can help provide a valuable first step.

Local governments represent such a huge diversity in terms of geography, population and resources. They range from

Future Appendices to the Local Government Information Security Getting Started Guide

This list will continue to evolve as necessary.

- Cyber Security Awareness resources
- How to use and install Firewalls
- Internet and Acceptable Use Policy
- Cyber Security Citizens' Notification Policy
- Templates for How to Perform Risk Assessments
- Roles and Responsibilities of the Designated Individual for Security
- How to Implement Information Security in Your Organization
- Passwords Standards
- Hardware/Software Asset Inventory Template
- How to Install Software Patches
- Guidelines for Backing-up Information
- How to Properly Dispose of Media and Equipment
- Incident Reporting Policy Templates

Instant Messaging (IM) The ability to exchange short messages online with co-workers or others. IM solutions can take several forms. They can use an existing *Internet* based service, or they can be an Intranet only solution implemented and controlled within an IT department. The latter is significantly more secure than the former, but lacks access to business partners. (NYS Information Security Policy)

PDAs- Personal Digital Assistants are small portable computing devices that may contain email, calendars, telephone and other personal information.

Software Patches People are constantly finding security holes (i.e. vulnerabilities) in computer software which could be used to infect your computer with a virus, spyware or worse. When vulnerabilities are discovered, the software 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 some one to try to exploit this security hole can be as little as a few days. (CSCIC Awareness brochure)

Spyware and related “adware,” are software sometimes downloaded from a web page, by following a link in an email or are installed with freeware or shareware software without the user’s knowledge. Spyware is used to track your Internet activity, redirect your browser to certain web sites or monitor sites you visit. Spyware may also record your passwords and personal information to send to a malicious web site. (CSCIC Awareness brochure)

URL Uniform Resource Locator: The Internet address of documents and other resources on the World Wide Web. It begins with <http://www> followed by the rest of the name of the resource. It is the common name for a site’s web page.

those with local government representatives who work out of their homes to local governments that are of the size and complexity of some states. Yet no matter what the size or complexity of the local government, we are all connected to one another and face the same threats. Therefore, all local governments need to be aware of the cyber threats, understand what their vulnerabilities and risks are and take appropriate steps.

While implementing good cyber security practices sounds daunting, this guide is your first step to a more secure environment. It is not intended to be an all inclusive and comprehensive approach to cyber security. It is more a first – but very important – step in the right direction.

This guide provides real actionable items for your local government to implement to enhance cyber security. More information will be forthcoming but for now **let’s get started**.

Why is Information Security Important?

Some examples of how your computer system could be affected by an information security incident — whether because of improper information security controls, manmade or natural disasters, or malicious users wreaking havoc include the following:

- Your websites could be disabled and unavailable for use by your citizens.
- The office computers that your employees use could be shut down by a virus.
- A hacker could break into one of your databases and steal the identity of your employees and citizens.
- A disgruntled former employee could manipulate or destroy important governmental data.

These and other information security incidents could certainly have a negative impact on your government.

The average unprotected computer connected to the Internet, even a solitary one sitting alone at home, can be compromised in less than a minute. An infected or compromised

computer connected to other unprotected computers can easily and quickly pass that infection, or function as a "*backdoor*" to the others.

Even a computer without Internet connections can be cause for information security concern. An unprotected machine may not prevent unauthorized individuals from accessing information contained within it. It may become infected through an infected inserted disk (floppy, CD or DVD) brought in from elsewhere. Information stored on it may be permanently lost due to accidental or intentional alteration or deletion. These are just a few examples of risks to information kept on any computer.

Information security incidents can cripple local government computers and cause a loss of public confidence. Inadequate information security measures can lead to the compromise of sensitive information about local government operations and its citizens. Government has a responsibility to its citizens and business partners, both public and private, to safeguard the information with which it is entrusted and to perform mission critical functions.

What is an Unprotected Computer?

An unprotected computer is one that does not:

- have antivirus or *spyware* protection software installed and updated regularly
- have installed hardware/software (such as a firewall) to manage communications between and among networks
- have an offsite back up of important files
- require the user to authenticate (using a password) when logging on or
- have operating system patches regularly installed on it

What are the Objectives of Local Government Information Security?

As custodians of information we in government have a responsibility to protect this information. The objectives below

Glossary Definitions for italicized words:

Backdoor is an unauthorized method into a computer device.

Back up (verb) to copy an electronic record to ensure its information will not be lost, often while compressing data to save space (SARA Disaster Recovery glossary)

Backup (noun) a copy of an electronic record, maintained to protect the information from loss and often compressed to save space (SARA Disaster Recovery glossary)

Denial of Service (DoS) is an attack that *successfully* prevents or impairs the authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. (NIST 800-61)

Firmware is software that is embedded into hardware; it can be updated and be accessed by the user.

Firewall a security system that uses hardware and/or software mechanisms to prevent unauthorized users from accessing an organization's internal computer network. (SARA Disaster Recovery glossary)

Any machine connecting to the Internet should utilize a firewall. There are two types of firewalls. Software firewalls usually run on PCs. Hardware firewalls are separate devices designed to efficiently protect computers. They are usually used by businesses, organizations, schools and governments. All firewall protection creates a barrier between the computers and the Internet. (CSCIC Awareness brochure)

Flash drives/thumb drives are very small portable storage devices that may store very large (gig) quantities of information and can be attached to a USB or firewire port quickly and easily to transfer files.

IT (Information Technology) is also known as Management Information Systems (MIS).

- for “sniffing” (i.e., monitoring network traffic) except for those authorized to do so as part of their job responsibilities

10. Take steps to securely dispose of storage media and equipment

Take steps to properly dispose of storage media and equipment. Hard drives and other disposable computer equipment may contain saved information even if that information has been “deleted.” Run utilities and/or physically destroy the hard drive to ensure it is clear.

Looking for More Information?

Visit the Multi-State Information and Sharing and Analysis Center (MS-ISAC) website (<http://www.cscic.state.ny.us/msisac/index.html>) for additional cyber security resources. You may also email the MS-ISAC at isac@cscic.state.ny.us.

You are on your way – CONGRATULATIONS!

provide a starting point for local governments in addressing their information security needs and developing their own internal procedures. Local governments must address information security and focus their efforts on accomplishing the following:

- Promote and increase the awareness and training of information security (DVDs, videos, PSAs, etc);
- Communicate the responsibilities for the organization and individual users’ protection of information;
- Identify risk and take appropriate action;
- Prepare for the inevitable – disaster recovery. Protect the availability and recoverability of the government’s information services and missions.

What is a Cyber Security Incident?

A cyber security incident is considered to be any adverse event that threatens the confidentiality, integrity or availability of an entity’s information resources. These events include but are not limited to the following malicious activities:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or *denial of service (DoS)*
- unauthorized use of a system for the transmission, processing or storage of data
- changes to system hardware, *firmware* or software characteristics without the local government’s knowledge, instruction or consent
- attempts (either failed or successful) to cause failures that may cause loss of life or significant impact on the health, mission or economic security of the local government and its citizens

What Must Be Done?

The most important message to convey is: “Information Security is everyone’s responsibility.” Each of us needs to protect information handled during our daily work.

Local governments frequently have multiple elected official

roles, part-time employees and hired information technology help attempting to meet the needs of constituents. With access to computers and information assets, all employees and officials need to understand their responsibilities for protecting the information they handle each day. Contractors must also understand their responsibilities, which should be delineated in the terms and non-disclosure agreements and contractor conditions in all contracts. Background checks where authorized may be useful as well.

Information security is an ongoing task initiated by the development of a security policy. Implementing a good security policy will establish roles and responsibilities and educate and inform all members of the local government.

Every organization should be implementing the following action items on a regular basis in order to help enhance your organization's cyber security readiness and response. This list is not all-inclusive, nor is it organized in any specific order, but will provide you with some minimum action steps to take.

TOP TEN CYBER SECURITY ACTION ITEMS

1. Designate a Principal Individual responsible for information security. Identify this individual's Roles and Responsibilities

- Designate, in writing, a principal individual who is responsible for information security in order to ensure that proper policies and procedures are in place. This may be a part-time or full-time assignment depending on the scope and complexity of the government's operations.
- Develop an information security plan.
- Ensure a hardware and software asset inventory is maintained.
- Determine which information assets require protection and put procedures in place to protect them.
- Develop back-up plans so that critical business can continue.

8. Implement training and awareness programs

Train everyone (elected officials, employees, volunteers, interns and contractors) who uses a computer to practice safe computing and follow the local government's policy.

Business Manager, End User and Technical Training modules are publicly available for local government use. The live training sessions were recorded and made available to State and local government for their cyber security training programs. You may email your request to security@cscic.state.ny.us. In addition, free cyber security webcasts are conducted every other month. For more information and to view archives of past webcasts, visit <http://www.cscic.state.ny.us/msisac/webcasts/index.htm>.

9. Develop Internet and acceptable use policy

When the organization's employees connect to the Internet using any organization's Internet address designation or send electronic mail using the organization designation, it should be for purposes authorized by organization management. The following is not an all-inclusive list, and provides only examples of behavior that could result in security breaches. Specifically, the Internet and electronic mail should not be used:

- to represent yourself as someone else (i.e., "spoofing")
- for spamming
- for unauthorized attempts to break into any computing system whether your organization's or another organization's (i.e., cracking or hacking)
- for theft or unauthorized copying of electronic files
- for posting sensitive organization information without authorization from the organization
- for any activity which could create a denial of service attack, such as "chain letters"

ensure account termination is performed (including such items as laptops, cell phones, *PDA*s, etc.). This applies not only to employees who have left the local government entity, but also to those who may have changed departments or job function within the locality and therefore may have different access to certain accounts.

7. Protect Information

- *Back up* information regularly. What should you back up? That depends on your information and the risk to the loss of that information. Store the backup media offsite; periodically test that the information can be reloaded from *back-ups*. Information that is not backed up can be lost, therefore, *backup* as often as possible to minimize the loss of information.
- Install operating system *software patches* regularly.
- Handle email and *instant messaging* with care.
- Don't click on links in e-mail. Type the *URL* in the browser bar.
- Don't open attachments that you didn't expect to receive.
- Delete email that directs you to a website where you are prompted to fill in personal information.
- Delete hoax and chain letter mail.
- Pay close attention to small portable devices such as disks, CDs, *flash drives*, *thumb drives*, *PDA*s. They can carry a lot of information, so be sure they do not get lost or misplaced.
- Be careful of Internet sites visited. Some sites may
 - redirect you to other sites that you did not intend to visit
 - request personal information that will be later used in identity theft
 - be sources of malicious activity

- Establish communication procedures so that everyone knows what, how and to whom to report an information security incident or problem.
- Be aware of regulations regarding the protection of information.

2. Know how to recognize that you might have a problem

A computer may have been compromised if it is...

- slow or non-responsive
- experiencing unexpected behavior such as programs popping up
- showing signs of high level of activity to the hard drive that is not the result of anything you initiated
- displaying messages on your screen that you haven't seen before
- running out of disk space unexpectedly
- unable to run a program because you don't have enough memory – and this hasn't happened before
- constantly crashing
- rejecting a valid and correctly entered password

Your organization may be experiencing a cyber security incident if it is...

- finding email refused (bounced back)
- no longer receiving any email or visitors to your web site
- receiving complaints from the users that their passwords don't work anymore
- getting complaints from the users that the network has slow response time

3. Understand how to deal with problems

- Determine if you have an information security problem.

- Take infected or compromised equipment out of service as soon as practical to prevent further harm.
- Notify management and other users as appropriate based on your local government information security policy.
- Consider notifying your partners with whom you connect.
- Contact your local law enforcement if you suspect a crime has been committed.
- Identify the types of information that you would want to gather during a cyber security incident:
 - o Organization name
 - o Point of contact name
 - o Phone/pager/cell
 - o Email
 - o Characteristics of incident
 - o Date and time incident was detected
 - o Scope of Impact
 - How widespread
 - Number of users impacted
 - Number of machines infected
 - o Nature of incident:
 - *Denial of Service*
 - Malicious code
 - Scans
 - Unauthorized access
 - Other
- Fix the problem and restore the compromised equipment to service.
- Reassess your security policy and practices to determine what lessons can be learned from the information security incident to help you strengthen your security practices.

4. Physically protecting Equipment

- Computer equipment must be physically protected from security threats and environmental hazards.

- If traveling with a laptop, never check it in at the airport; keep it with you at all times or in a secure location.
- Use a surge protector that has power and telephone connections.
- Access to devices may need to be controlled based upon job function.

5. Protect Essential Hardware/Software

- Install and use a *firewall*. Set your computer to automatically check for new updates.
- Set your computer to auto-update to ensure you have the latest security *patches* applied to your computer.
- Install *spyware* and virus protection software and update regularly. (A *firewall* does not substitute for anti-virus software.)

6. Control Access

- Each user must have a unique login (userid) and password.
- Establish good passwords – at a minimum, a combination of eight alpha and numeric characters; avoid the use of commonly used words especially family names or other words that can be readily associated with you.
- If a computer is located where unauthorized staff or public have access, make sure the screen is not in view.
- “Lock” computers when they are unattended so upon the user’s return they are prompted to enter their userid and password. (Generally, control+alt+delete and/or set computers to automatically lock.)
- Don’t set the option that allows a computer to remember any passwords.
- Implement an employee departure checklist to