Cyber Security

Getting Started

A Non-Technical Guide

Essential for Executives and Managers

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

**U.S. Department of Homeland Security
National Cyber Security Division**

This Guide has been endorsed by the following:

The Global Council
http://www.csocouncil.org/

Public Safety and Security
http://www.psitec.org

National Cyber Security Alliance
http://www.staysafeonline.info/

National Association of Counties
http://www.naco.org

ISAC Council
http://www.isaccouncil.org/

Water ISAC
http://www.waterisac.org/

Surface Transportation and Public Transportation ISAC
http://www.surfacetransportationisac.org

Communications ISAC
http://www.ncs.gov

Financial Services ISAC
http://www.fsisac.com/

IT ISAC
http://www.it-isac.org/

Research and Education Networking ISAC
http://www.ren-isac.net

Emergency Management and Response ISAC
http://www.usfa.fema.gov/fire-service/cipc/cipc-new.shtm

Special thanks and appreciation to the following individuals 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 Shuart**, 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 Lohrmann** from Michigan, **Chris Turpin** from North Carolina and **Elayne Starkey** from Delaware.

THANK YOU!

Future Appendices to the Cyber 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

Dear Executives and Managers,

*Welcome to the **"Cyber Security: Getting Started Guide,"** and congratulations on taking an important step in furthering your knowledge and awareness regarding cyber security.*

Because cyber security knows no geographic boundaries, the information contained in this Guide is applicable to public and private organizations throughout the nation. 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. We recommend distribution to all executives and managers in your organization. It should also be shared with those who implement your information technology as well as with the individual(s) responsible for cyber security in your organization.

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

William F. Pelgrin
Director
NYS Office of Cyber Security and
Critical Infrastructure Coordination

and

Chair
MS-ISAC

Cyber Security: Getting Started

This guideline is intended for executives and managers in public and private organizations. It is designed to demystify cyber security and to provide a clear, concise and achievable approach to improve an organization's cyber security posture.

Cyber security can seem overwhelming to many. When you hear statistics that thousands of new computer *viruses** are reported each 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 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.

Cyber security is a basic concept. As leaders of your organization, you are responsible for protecting the information in your care. Cyber security is a business function, and technology is a tool that can be used to more securely protect information assets. While addressing cyber security may seem like a daunting task, it is much more palatable if taken in manageable chunks. Cyber 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*, intrusion detection and prevention systems, anti-*virus* and anti-s*pyware* 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, effective and sustainable cyber security program. This guide can help provide a valuable first step.

Regardless of the size or complexity of the organization, we are all connected to one another and face the same threats.

*Words in italics can be found in the glossary in the back of this Guide.

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.

PDAs (Personal Digital Assistants)**—**small portable computing devices that may contain email, calendars, telephone and other personal information.

Software Patches— fixes to correct a problem. 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 someone to try to exploit this security hole can be as little as a few days.

Spyware (and related "adware")**—**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.

URL (Uniform Resource Locator)—the Internet address on the World Wide Web. It usually 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.

Virus—a self-replicating program that spreads by inserting copies of itself into other programs.

Glossary Definitions for italicized words:

Backdoor— 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.

Backup (noun)**—**a copy of an electronic record, maintained to protect the information from loss and often compressed to save space.

Configure— to choose options in order to create a custom system.

Denial of Service (**DoS**)**—** 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.

Firmware—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.

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.

Flash drives/thumb drives—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)—also known as Management Information Systems (MIS).

Therefore, all organizations need to be aware of the cyber threats, understand what their vulnerabilities, risks and consequences 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 steps your organization can take to enhance cyber security. More information will be forthcoming but for now **let's get started**.

Why is Cyber Security Important?

Some examples of how your computer system could be affected by a cyber security incident — whether because of improper cyber 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 users.
- 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 customers.
- A disgruntled former employee could manipulate or destroy important organizational data.
- A malicious user could use your systems to attack other systems.

These and other cyber security incidents could certainly have a negative impact on your organization.

The average unprotected computer connected to the Internet 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 an Internet connection can be cause

for cyber 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, flash/USB drive 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 threats to information kept on any computer.

Cyber security incidents can cripple computers and cause a loss of public confidence. Inadequate cyber security measures can lead to the compromise of sensitive information about organizational operations and its customers. An organization has a responsibility to its customers and business partners, both public and private, to safeguard the information with which it is entrusted and to perform its business 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
- have operating system patches installed and regularly updated

What are the Objectives of a Cyber Security Program?

As custodians of information, organizations have a responsibility to protect this information. The objectives below provide a starting point for organizations in addressing their cyber security needs and developing their own internal procedures:

- Promote and increase the awareness and training of cyber security (DVDs, videos, Public Service Announcements, etc);

Cyber Security Tasks Quick Reference Checklist

This checklist is intended to help the designated person(s) responsible for information security in their organization to determine minimally how frequently a task should be done. Some tasks are done daily while others occur weekly, annually or as needed.

• Update anti-virus software	daily
o Automate updates if possible	
• Update spyware software	daily
• Update operating software	daily
• Back up files	daily
o Incremental back ups	daily
o Full back-up weekly & stored off-site	weekly
• Conduct security review (Annual Report)	annually
• Establish and review inventory (hardware/software)	annually
o Information assets/applications etc.	as acquired
• Change staff access control	as it happens
• Draft non-disclosure agreements	at start of agreements
• Inform vendors of security requirements	at start of agreements
• Train staff on Acceptable Use	start of employment/ repeat annually
• Hold user awareness training	start of employment/ repeat annually
• Update and review policies	reviewed annually
• Revise Policies	as needed
• Notify users of alerts, advisories	daily

- 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"
- 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.msisac.org) and the US-CERT website (http://www.us-cert.gov/) for additional cyber security resources. You may also email the MS-ISAC at isac@cscic.state.ny.us.

You are on your way to better cyber security
CONGRATULATIONS!

- Communicate the responsibilities for the organization and individual users' protection of information;
- Identify threats, vulnerabilities and consequences and take appropriate action;
- Prepare for the inevitable – disaster recovery. Protect the availability and recoverability of the organization'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 organization'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 organization and its customers

What Must be Done?

The most important message to convey is: "Cyber Security is Everyone's Responsibility."

With access to computers and information assets, all employees 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 non-disclosure agreements and contractor conditions in all contracts. Background checks for individuals in critical or sensitive cyber security, information technology, or management positions should be conducted.

Cyber security is an ongoing task initiated by the development of a security policy. Implementing a good security policy will establish roles and responsibilities, educate and inform all members of the organization and ensure that procedures follow established practices for a sustainable program.

Every organization should be implementing the following action items on a regular basis in order to help enhance their 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 Cyber Security

- Designate, in writing, a principal individual who is responsible for cyber 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 organization's operations.
- Identify this individual's roles and responsibilities.
- Develop a cyber 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 procedures for responding to cyber security incidents.
- Develop back-up plans so that critical business functions can continue.
- Implement a cyber security awareness and training program.
- Establish communication procedures so that everyone knows what, how and to whom to report a cyber security incident or problem.

8. Implement Training and Awareness Programs

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

Business Manager, End User and Technical Training modules are publicly available at the following website: www.msisac.org/awareness/video. In addition, free cyber security webcasts are conducted every other month. For more information and to view archives of past webcasts, visit www.msisac.org and select "National Webcast Initiative."

9. Develop Internet and Acceptable Use Policy

When the organization's employees connect to the Internet or send e-mail using the organization's resources, it should be for purposes authorized by the organization. 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

PDAs, etc.). This applies not only to employees who have left the organization, but also to those who may have changed departments or job function within the organization 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 *backups*. Information that is not backed up can be lost, therefore, *back-up* 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 email. 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 email.
- Pay close attention to small portable devices such as disks, CDs, *flash drives, thumb drives, PDAs.* 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 do the following:
  - 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

- 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 website
- 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 a cyber 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 organization's cyber 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:
  - Organization name
  - Point of contact name
  - Phone/pager/cell
  - Email
  - Characteristics of incident
  - Date and time incident was detected
  - Scope of Impact
    - How widespread
    - Number of users impacted
    - Number of machines infected
  - 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 cyber 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, *configure* 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 regularly update. (A *firewall* does not substitute for anti-virus software.)

6. Control Access

- Each user must have a unique login (userid) and password to provide accountability and limit access to appropriate functions.
- 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 ensure account termination is performed (including such items as laptops, cell phones,