Cyber Security

Getting Started:
A Non Technical Guide

MS-ISAC

Multi-State
Information Sharing & Analysis Center™

A DIVISION OF Center for Internet Security

For additional copies or to download this document, please visit:

http://msisac.cisecurity.org/resources/guides

The information in this document is provided by the Multi-State Information Sharing and Analysis Center (MS-ISAC), a division of the Center for Internet Security (CIS), for non-commerical informational and educational purposes only. CIS does not warrant the accuracy or completeness of the information or commit to issue updates or corrections to the information. CIS is not responsible for any damages resulting from use of or reliance on the information contained herein.

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 of cyber security.

Because cyber security knows no geographic or demographic boundaries, the information contained in this Guide is applicable to public and private organizations throughout the nation.

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
Founder and Chair, MS-ISAC
President and CEO, Center for Internet Security

The Center for Internet Security (CIS) is a nonprofit organization focused on enhancing cyber security readiness and response. CIS works through four complementary divisions - Security Benchmarks, Multi-State ISAC, Trusted Purchasing Alliance, and the Integrated Intelligence Center. Each division offers high-quality, timely products and services to help partners achieve security goals through expert guidance and cost-effective solutions. With a commitment to excellence through collaboration, CIS acts as a trusted central resource for cybersecurity in the private and public sectors.

Introduction

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

Cyber security can seem overwhelming to many. When you hear statistics that thousands of new types of malicious software* 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 constantly 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.

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, antivirus 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 implement 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.

This guide is not intended to be an all inclusive and comprehensive approach to cyber security. It is a first and a very important step in the right direction. It provides real actionable steps your organization can take to enhance cyber security. Let's get started.

Cyber Security Objectives

The objectives below provide a starting point for addressing cyber security needs and developing internal procedures.

A cyber security program should:

- promote and increase the awareness and training of cyber security
- 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, including protecting the availability and recoverability of the organization's information services and missions

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 compromised and/or unavailable to your users.
- The office computers that your employees use could be shut down by malicious software.
- Someone could break into one of your databases and steal the identity of your employees and customers.
- A disgruntled 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.

An unprotected computer is one that does not:

- have antivirus or spyware protection software installed and updated regularly
- have installed hardware or sofware firewall to manage communications between and among networks
- require the user to authenticate (using a password or a token) when logging on
- have operating system and software patches installed and regularly updated

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 along that infection, or function as a “backdoor” to your network.

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 device or media (CD, flash/USB drive or DVD) brought in from elsewhere. Information stored on the computer 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. An oganization has a responsibility to its customers and business partners, both public and private, to safeguard the information with which it is entrusted.

What Should I do to be Cyber Secure?

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 your 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.
- Be aware of regulations regarding the protection of information.

Know How to Recognize 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 it doesn't have enough memory – and this hasn't happened before
- constantly crashing
- automatically communicating with external computers for which there is no authorized or business need
- receiving bounced-back emails

Other indicators that something is wrong could include your organization:

- is no longer receiving any email or visitors to your website
- is receiving complaints from the users that their passwords don't work anymore
- is getting complaints from the users that the network has slow response time
- is getting complaints from users that their computers are being infected when they visit your website

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.
- Fix the problem (or partner with a trusted provider to assist) 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.

Physically Protect 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.
- Physical access to devices needs to be controlled.

Protect Essential Hardware/Software

- Install, configure and use a firewall.
- Set each computer to auto-update to ensure it has the latest security patches applied, or institute a patch management solution within your organization.
- Install spyware and virus protection software and regularly update. A firewall does not substitute for anti-virus software.

Control Access

- Each user must have a unique login (userid) and password to provide accountability and limit access to appropriate functions.
- Establish good passwords. Passwords should have at least ten characters and include uppercase (capital letters) and lowercase letters, numbers and symbols. 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, you can lock by hitting 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, 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.

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, backup as often as possible to minimize the loss of information.
- Install operating system and software patches regularly.
- 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

Develop Internet and Acceptable Use Policy

When the organization’s employees connect to the Internet or send email 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 email 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” for “sniffing” (i.e., monitoring network traffic)

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.

Take Steps to Securely Dispose of Storage

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 of sensitive, private or personal information.

Task Quick Reference Checklist

This checklist is intended to help the designated person(s) responsible for information security in the 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 antivirus software. Automate updates if possible	Daily
Update spyware software	Daily
Update operating system and software	On a regular schedule, as patches are released.
Back up files	Daily
Perform incemental back ups	Daily
Perform full back ups	Weekly
Conduct security review	Anually
Establish and review inventory (hardware/software)	Anually/As acquired
Change staff access control	As needed and when job function changes.
Draft non-disclosure agreements	Start of agreements
Review policies	Annually
Revise policies	As needed
Notify users of alerts / advisories	Daily or as needed

Glossary

Backdoor – an unauthorized method into a computer device.

Back up – to copy an electronic record to ensure its information will not be lost, often while compressing data 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 networks and computers. They are usually used by businesses, schools, governments, and other organizations, as opposed to home users. 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 other port (such as firewire) to quickly and easily transfer files.

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

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.

Malicious Software – software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

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

Software Patches – software thats correct a problem. Security holes (i.e. vulnerabilities) in computer software can enable attackers 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.

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 website.

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.

Looking for More Information?

Visit the Multi-State Information and Sharing and Analysis Center (MS-ISAC) website (http://www.msisac.org) and the StopThinkConnect website (http://www.stopthinkconnect.org) for additional cyber security resources.

You may also email the MS-ISAC at info@msisac.org.

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

For additional copies or to download this document, please visit:

http://msisac.cisecurity.org/resources/guides