National Campaign
for
Cyber Hygiene
Count, Configure, Control, Patch, Repeat

TOOLKIT
for
COUNT

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

Introduction

In this digital age, we rely on our computers and devices for so many aspects of our lives that the need to be proactive and vigilant to protect against cyber threats has never been greater. However, in order to be as secure as possible, we need to **use good cyber hygiene** - that is, making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices.

The Campaign, a joint effort of the Center for Internet Security (CIS) and the Governors Homeland Security Advisors Council (GHSAC), aims to create a nationwide movement toward measurable–and sustainable–improvements in cybersecurity.

The Cyber Hygiene Campaign is a multi-year effort that provides key recommendations for a low-cost program that any organization can adopt to achieve immediate and effective defenses against cyber attacks.

The Campaign has developed toolkits for each of its key recommendations to provide easily understood instruction sheets and information for entities to improve their cybersecurity posture. The toolkits are: Count, Configure, Control, Patch and Repeat. These toolkits are dynamic documents and will continue to evolve to meet the ever-changing cyber threat landscape. In addition, a unique Executive Measurement Guide will be issued to assist Executives in the implementation of the toolkits.

For more information about the Cyber Hygiene Campaign, and to access electronic versions of the toolkits, please visit the Campaign website at: http://www.cisecurity.org/about/CyberCampaign2014.cfm

Join the cause and show your commitment to getting cyber healthy by signing the online pledge! Take the Cyber Hygiene Pledge: www.cisecurity.org/cyber-pledge

Special thanks to the following individuals who were instrumental in the development of the toolkits:

- Jonathan Trull, Chief Information Security Officer
  Qualys, Inc.
- Deborah A. Snyder, Acting Chief Information Security Officer
  NY State Office of Information Technology Services
- Gary Coverdale, Assistant CIO/CISO
  Information Technology Services, Napa County, California
- Members of the Cyber Hygiene Panel

Center for Internet Security

Homeland Security Advisors Council

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

Table of Contents

I. Plain English Guide for Count

II. Technical How-To Guide for Count

III. How to Measure Guide for Count

IV. Additional Resources for Count

V. Mapping to NIST Cybersecurity Framework for Count

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

I. Plain English Guide for Count

Basic Questions to Better Cyber Security Hygiene

Cyber Hygiene Priority -- Count: Know what's connected to your network

1. Why is this step important?

- Cybersecurity begins with knowing what is connected to your network.
- To identify the existence of authorized and unauthorized devices and lost or stolen assets, you need to begin with an inventory.
- Knowing what IT assets you own will allow you to better manage your IT infrastructure and its security.
- Every piece of equipment has vulnerabilities and exposes you to risk. How you handle the risk will depend on what the equipment is and what purpose it has.
- You can't protect what you don't know exist.

2. What to do?

Count (inventory) and document the type of device, its location and the assigned owner of your organization's IT assets. These assets include all your:

- Computers, laptops, tablets;
- Smart phones, PDAs;
- Thumb drives, removable hard drives;
- Printers;
- Routers, switches; and
- Servers.

Start small and grow.

- Start with counting your computers, laptops and tablets.
- Physically locate and tag each piece of equipment – buy numbered (barcoded) tags with your organization's name on it and affix to each device.
- As you tag, log identifying information about each piece of equipment.
- For each computer, for example, the identifying information includes the make, model, serial number, the computer's hard drive size, and the amount of memory.
- Initially establish and maintain a log for an instantaneous "at a glance" understanding of your organizations IT assets. See log template included in the Resources section.
- Over time you will want to automate this process so that you can keep tabs continuously on what you have, where it is and who has it. (In the future, guidance will be provided on how to automate this process and to develop a dashboard, but for now just get going.)
- Develop a written policy that requires the creation and maintenance of a complete and accurate IT asset inventory.
- Senior executives in your organization should review the inventory at least yearly, reconcile any discrepancies and discuss the security of the assets.

3. Who should be responsible to do this?

No two organizations are exactly alike. Some have CIOs, others CISOs, still others have CTOs, and some even have EIEIOs. Whoever in your organization has responsibility for installing and maintaining your IT equipment and systems should have the lead for conducting the inventory of your IT assets and for maintaining a process to ensure the count stays accurate. If you don't have an IT person, identify someone who is organized and responsible to do the inventory.

4. When to do it?

The inventory can be conducted at any time during the year – the timing should be based on what works best for you. Depending on the size of your organization, allocate anywhere between a couple of days (small entities), couple of weeks (medium entities), couple of months (large entities) to conduct the initial inventory. Thereafter, reconcile your inventory of assets at least once a year (and, of course, add to your inventory as new equipment is deployed).

5. Where to start?

Actually, this doesn't matter. It is more important to just start. Set up a schedule by departments or functional areas and begin.

In larger organizations, plan for a "shotgun" start – that is, begin counting in multiple parts of the organization at once. Establish points of contact in each office or section of the organization to ensure access to the devices to be inventoried.

Set realistic deadlines to complete the inventory and stick to them.

6. How to do it?

To find Computer Information to view detailed information about your computer's hardware and software, examine diagnostic information, and other information needed for your inventory, perform the following steps:

Windows Devices:

- Open Help and Support Center
- Click Tools
- Click My Computer Information

Apple Devices:

- Click on the Apple Icon (upper right hand corner)
- Go to "About this Mac"

Window screen shot

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

II. Technical How-To Guide for Count

Tasks to consider

Tasks Included in level	**LOE (Level of Effort - resources, effort ,cost)** High Med, Low	**Priority** How important is it for implementation of security program/controls (High Med, Low)	**Completion Criteria**
Create and maintain a master database/log of H&S found on company networks/devices.	High	High	All devices are counted and documented on the master database, including: • Computers, laptops, tablets; • Smart phones, PDAs; • Thumb drives, removable hard drives; • Printers; • Routers, switches; and Servers.
Deploy an automated asset inventory discovery tool. It should be used to build an asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	Med	High	Automated tools and processes implemented. Scans/audits occurring at least monthly.
Identify and document the number of outbound paths to the Internet. Ensure all paths are authorized and transit through approved security devices (i.e., firewall, web filter, IDS, IPS)	Low	Med	Paths documented in writing and formally approved by security.
Develop and implement controls that both (1) prevent the use of unauthorized H&S and (2) quickly identifies and removes unauthorized H&S, if found	High	High	Combination of preventive & detective controls identified, authorized by management, an implemented. Controls implemented on 90%+ of all networks & assets.

Resources:

Include: Links to resources (templates, etc), automated tools that are free or low cost (such as nmap), Training options for the tools or content area (online tutorials, etc), mentoring options (this needs to be developed)

For ideas on conducting an IT asset inventory see the following links:

Resources	Link
Nmap/ZenMap How to Guides; download tool	http://nmap.org/docs.html
Common default passwords	
CIS Benchmarks / CIS-CAT	
DoD STIGS	
Qualys Browser Check	
PRADS	

Sample Hardware Inventory Log to consider:

TECHNOLOGY INVENTORY -- HARDWARE

Macon County Board of Education

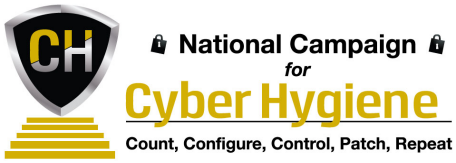
Employee Name: _____

Employee Position: _____ **School or Location:** _____

Date: _____ **Room #** _____

Hardware DESCRIPTION (Include all computers, monitors, printers, scanners, digital cameras, copy machines, etc. AND the Model name or number)	NUMBER (for example: M -- #2 MCHS)	Serial Number	Purchase Date	Funding Source (Grant, Local Technology Funds, E-Rate, SPED, Title I, etc.)	COST	Internet Connection (Yes or No)	Microsoft Office 2000/XP/2003 License	CD	Windows 98/XP CD	
example below:										
Computer,Gateway,P4,WIN XP, 3.0 GHZ	C--#2 RBS	SN--9900107054	Jul-06	Local Tech.	$1,065	Yes	2003	CD	XP	CD

Created by Patricia Ferguson *9/3/2011* *School Hardware Inventory Sheet a45c9b7a-6a06-4ca0-9de1-c637d8f73c0c.xls*



III. How to Measure Guide for Count

1) How often does your hardware inventory/asset database get updated?
2) How long does it take to detect new devices added to the organization's network (time in minutes)?
3) How long does it take to detect new software installed on systems in the organization (time in minutes)?
4) How long does it take to alert the organization's administrators that an unauthorized device is on the network (time in minutes)?
5) How long does it for the organization's administrators to detect that an unauthorized software application is on a system (time in minutes)?
6) How long does it take to isolate/remove unauthorized devices from the organization's network (time in minutes)?
7) Are administrators able to identify the location, department and other critical details about the unauthorized system that is detected (yes or no)?
8) Are the scanners able to identify the location, department and other critical details about the unauthorized software that is detected (yes or no)?

IV. Additional Resources for Count

The Cyber Hygiene Toolkits are dynamic documents and will continue to evolve to meet the changing cyber threat landscape. In addition, a unique Executive Measurement Guide will be issued to assist Executives in the implementation of the toolkits.

For more information about the Cyber Hygiene Campaign, and to access electronic versions of the toolkits, please visit the Campaign website at: http://www.cisecurity.org/about/CyberCampaign2014.cfm

If you have expertise, resources or information relating to any of the following areas that you could share for subsequent editions of the toolkits, **please contact us at 518.880.0699 or contact@cisecurity.org**:

- Case Studies
- Webcasts, Podcasts, Videos [e.g., YouTube]
- Mentor Programs [to pair experienced individuals with those looking to gain more expertise]
- Upcoming Events [trainings, conferences, roundtable discussions]
- Other

V. Mapping to NIST Cybersecurity Framework for Count

"Count" maps to the following NIST Framework function(s) and Subcategories:

NIST Framework Function	Subcategory(s) / Description(s)
Identify	**Asset Management** D.AM-1: Physical devices and systems within the organization are inventoried
	Asset Management ID.AM-2: Software platforms and applications within the organization are inventoried