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

TOOLKIT
for
CONFIGURE

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®

Governors Homeland Security Advisors Council

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

Table of Contents

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

I. Plain English Guide for Configure

Basic Questions to Better Cyber Security Hygiene: Configure

Cyber Hygiene Priority -- CONFIGURE:
Protecting your systems by implementing key security settings.

1. **Why is this step important?**
   Many breaches occur because of mis-configured or poorly configured systems, e.g., the administrator and/or guest default passwords were not changed and are readily known by attackers. Without changes, the standard configurations that come installed by default on most computers and servers are not secure. Configuring devices using a few simple and easy steps can reduce the risk of compromise.

2. **What to do?**
   - Plan your configuration management program
     - assign roles and responsibilities for each phase of the configuration management process and establish appropriate policies and procedures.
   - Identify and implement configurations
     - develop, review, approve and implement secure baseline configurations for each type of asset.
   - Control configuration changes
     - develop processes such that all changes are formally identified and/or proposed, reviewed, analyzed for security impact, tested and approved prior to implementation.
   - Monitor
     - continuously monitor all IT assets to identify undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes and then work to bring those systems back into compliance with the approved security configuration baseline.

3. **Who should be responsible to do this?**
   Typically, the CIO or equivalent head of IT will be primarily responsible for designing and implementing a configuration management program. In addition to the CIO, the business owner of each asset and IT security staff will participate in developing the initial secure configuration baseline and reviewing and authorizing future changes to the baseline. In smaller organizations, all of these functions could be performed by the same person.

4. **When to do it?**
   Before deploying any new asset into production, IT should configure the asset according to the baseline security configuration settings approved by management. Once an asset is deployed into production, IT staff should use an automated tool to perform monthly or more frequent scans to identify and remediate any unauthorized changes found. In

addition, a change control board should be established that meets periodically to review requested changes to the secure configuration baseline. The change control board is typically composed of key IT and business staff (e.g., architects, security specialists, compliance analysts) and is responsible for reviewing and approving all changes before they are made to the secure configuration baseline.

5. **Where to start?**
   As with most things related to cyber security, it is essential that you start with your most critical assets first, including those systems that have administrative access to critical data and systems. As an example, if you process credit cards as part of your business, it would be advisable that you first develop and implement secure configuration baselines for all point-of-sale (PoS) systems and any systems that have direct, administrative access to the PoS systems. In addition, cyber criminals are continuously targeting systems that are exposed to the Internet and provide remote administrative services, such as Microsoft's and Apple's remote deskdop applications.

6. **How to do it?**
   - Using the "Count" toolkit, identify all of the different types of hardware and applications currently running within your business. Focus first and foremost on operating systems.
   - Research and select a well known and trusted secure configuration baseline for each type of hardware and application – examples include the Center for Internet Security's Benchmarks, National Security Agency's Secure Configuration Guides and the Defense Information Systems Agency's Security Technical Implementation Guides (STIGs).
   - Create a "gold image" for each type of asset using the above selected trusted secure configuration guidelines. A "gold image" is basically a template for quickly configuring existing and new IT assets based on the selected secure configuration baseline.
   - For all new IT systems and/or assets, ensure that IT staff use the "gold image" to configure the assets before moving them into production.
   - Establish a change control board that includes, at a minimum, a knowledgeable staff person who can review requested changes to determine the impact that such changes would have on both the security of the individual system and the overall network. Create policies and procedures that support the roles and responsibilities of the change control board, management, and those requesting changes to the secure configuration baseline.
   - Deploy an automated tool to continuously scan and assess all of the business' IT assets against the "gold image." All deviations should be identified and routed for remediation based on the importance of the asset and the significance of the mis-configuration.
   - For existing systems that were deployed prior to implementation of a configuration management program, develop a remediation plan to bring assets into compliance with the "gold image." Begin with the business' critical assets or those systems with administrative access to critical assets.

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

II. Technical How-To Guide for Configure

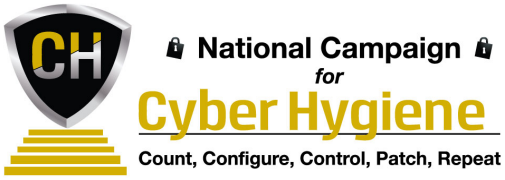
Tasks to consider

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
Establish a plan for rolling out secure configurations.	Low	Low	Plan established.
Identify a secure configuration baseline for each type of asset and implement configurations.	High	High	Secure images built for each category of asset.
Control configuration changes through a change control board and by removing and/or limiting those with administrative privileges.	Low	Med	Change control board in place and operating.
Monitor the configuration of all devices and remediate any deviations.	High	High	All assets are monitored at least monthly and 90%+ are configured properly.

Resources:

For technical guidance on securely configuring computer systems, see the following links to resources:

Resources	Links
SP 800-128	http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf
CIS Benchmarks	http://benchmarks.cisecurity.org/
DoD/Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/
Microsoft Baseline Analyzer	



III. How to Measure Guide for Configure

The single best measure for assessing configuration status is the percentage of total IT assets that comply with the industry-accepted configuration baseline. The measure can be calculated as follows:

- ((Total IT Assets – IT Assets Improperly Configured) / Total IT Assets) * 100

When first starting out, it may be helpful to set a more moderate threshold for systems that are categorized as meeting the secure configuration baseline. A secure configuration baseline typically includes hundreds of individual configuration items. A more moderate threshold may be that any system meeting 75% or more of the individual configuration items is scored as compliant.

It may also be helpful to track the percentage of compliant systems by business unit, system administrator, or type of technology. This information will help you better identify problem areas and best practices that can be shared throughout your organization.

IV. Additional Resources for Configure

The Cyber Hygiene 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, 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]
- Upcomming Events [trainings, conferences, roundtable discussions]
- Other

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

V. Mapping to NIST Cybersecurity Framework for Configure

"Configure" maps to the following NIST Framework Function(s) and Subcategories:

NIST Framework Function	Subcategory(s) / Description(s)
Protect	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained.
Protect	**PR.IP-3:** Configuration change control processes are in place.