National Campaign
for
Cyber Hygiene

Count, Configure, Control, Patch, Repeat

TOOLKIT
for
REPEAT

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

I. Plain English Guide for Repeat

Basic Questions to Better Cyber Security Hygiene

Cyber Hygiene Priority -- REPEAT: Protecting your systems by keeping current!

The top priorities for better Cyber Health (Cyber Hygiene) are:

- ***Count:*** Know what's connected to and running on your network.
- ***Configure:*** Implement key security settings to help protect your systems.
- ***Control:*** Limit and manage those who have admin privileges to change, bypass, or override your security settings.
- ***Patch:*** Regularly update all apps, software and operating systems.
- ***Repeat:*** Regularize the Top Priorities to form a solid foundation of cybersecurity for your organization.

Repeating each top priority 'item' is tantamount to a more effective security maturity. This is a 'cycle of events' that must repeat itself frequently enough when appropriate.

1. **Why is this step important?**
   Reviewing your 'Repeat' list will insure that each cycle of each individual priority has been appropriately met and that nothing falls through the cracks in your Cyber Health maturity.

2. **What to do?**
   The 'repeat' process will be applied depending on which priority is being considered but as a whole the repeat process must be done cyclical to insure that these high priority items are appropriately covered and applied to your enterprise.

- **Count**
  - this is an ongoing process in that every time an addition to hardware and software is added to your technical asset environment, it is added to your Count or Inventory. To insure that assets are actually added, a monthly or quarterly audit (manual or automated) should be done to insure that additional hardware or software hasn't been added to your Count which could bypass the **configuration, control,** and **patch** processes.

- **Configure**
  - Periodically review your configurations of all key technology assets.

- **Control**
  - Periodically review your access to key or protected systems and protect against unauthorized access to technology assets (including critical data).
- **Patch**
  - Make sure that your weekly and monthly patch process is occurring and appropriately applied to protect your technology assets (hardware and software).
- And…
  - **REPEAT**!

3. **Who should be responsible to do this?**
   Responsibility in insuring that an appropriate REPEAT process is occurring will be your CISO, CIO, or other management staff that can oversee that the Top Priorities for better Cyber Health is occurring within your organization.

4. **When to do it?**
   As each 'priority' is occurring cyclically (Patching may occur weekly, Count monthly or quarterly) an appropriate 'Repeat' process should be reviewed monthly or quarterly to adequately determine that 'total coverage' of your Cyber Health landscape is appropriate and at its highest level.

5. **Where to start?**
   Start with each Cyber Health toolkit and as you apply these toolkits to better protect your technology environment, develop a 'Repeat' process that will act as an insurance 'wrapper' around each Top Priority's individual cycle.

6. **How to do it?**
   Review, with your security and technology teams, each Top Priority. Develop a plan to review and insure that all cycles within each Priority item are done on a timely basis. Then schedule the repeating occurrence monthly or quarterly as a 'preset' time of month or quarter so that a review of each Priority isn't missed. This will allow for management oversight to insure that your Cyber Health processes are consistently, appropriately, AND timely applied.

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

The Repeat Cycle