NATIONAL CYBER SECURITY AWARENESS MONTH

SPOTLIGHT

Mr. Kyle Tucker, Jr.

TITLE: Technical Management Director Cyber/NH-2210-IV/PM I3C2

HOW LONG AT PEO EIS: March 2001

AWARDS / EDUCATION / OTHER ACHIEVEMENTS TO NOTE: First Federal Computer Week Rising Star winner PEO EIS, October 2006; ***Education:*** Masters degree, Certified Information Systems Security Manager (ISC2), Certified Information Systems Manager (ISACA)

1. WHAT DO YOU DO AND WHY IS IT IMPORTANT TO THE SOLDIER?

I support the Assistant Product Manager for Defensive Cyberspace Operations Infrastructure (DCO-I) in the acquisition of various DCO-I capabilities. I work with vendors to understand what is currently leading edge technology, as well as bleeding edge technologies that would benefit the Army's efforts in the new warfighting domain of cyber. We are currently engineering, furnishing, installing, securing, testing (EFIS&T) and deploying both enterprise and deployable solutions for Army Cyber teams.

2. WHAT ABOUT CYBER SECURITY INTERESTED YOU?

Then progression of the technology over time has fascinated me. I remember the visualization of the internet with browsers such as Mozilla, the ease of use brought about with Prodigy and America Online, the ability to move about, learn and communicate with people all over the globe from the comfort of your home fascinated me. I also remember having to explain to my parents about my computer's first virus and having to clean it up in a time when antivirus programs did not really exist yet using a DOS command line. Cyber is today's commercialized term, much like cloud. Anyone who has watched Star Trek has watched those systems, such as monitors, become high definition flat screen TV's. Communicators become cell phones, fax machines, etc. We watch our adversaries hack our systems today much in the same way Captain Kirk hacked the USS Reliant shield system to lower them in order to launch a successful counter attack.

3. IN YOUR OPINION, WHAT IS THE FUTURE OF CYBER SECURITY?

Improving the competency of the average person sitting behind the computer or rather solving the carbon problem. High speed internet is the new open door. We need to raise the minimum level of computer knowledge for most people so they understand how to at least keep their internet front door protected. As they connect the Internet of Things (IoT) devices to their bandwidth they must learn to secure those devices or add their voice to the small group who is recommending to vendors to keep firmware updated, and have the software interfaces tell the user to change default passwords before allowing someone to set up a wireless camera, router, baby monitor, fridge, etc. Failure to do this and we will continue to see these IoT devices be used for more Distributed Denial of Service Attacks.

4. ADVICE FOR KEEPING OUR INFORMATION SAFE IN THE DIGITAL AGE?

Keep a piece of painters tape over your laptop or web cams. External hard drives are dirt cheap so I recommend purchasing a three or more terabyte drive to store your photos, documents and files. Connect it to your network when you need to store something. Disconnect it when you are done. Understand that once something goes into the cloud you really do not have any control over it. If one hacker gets in and exfiltrates your information- it is over. Also, just as you should be checking your credit reports yearly, go to ***https://haveibeenpwned.com*** about every six months to check all of your email addresses. If an email address goes from green to red then change the password. And do not reuse passwords across accounts.

US ARMY PEO EIS
PEO Enterprise Information Systems

U.S. ARMY