Monthly Cybersecurity Newsletter

October 2017 Issue

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

---

National Cyber Security Awareness Month (NCSAM)

This October was the 14th year of National Cyber Security Awarensss Month (NCSAM), an annual campaign designed to raise awareness about the importance of cybersecurity. The Internet touches almost every aspect of everyone's daily life, whether we realize it or not. NCSAM is designed to engage and educate public and private sector partners through events and initiatives in order to raise awareness about the importance of cybersecurity. It also seeks to provide individuals with tools and resources needed to stay safe online, and increase the resiliency of the Nation in the event of a cyber incident. The themes for NCSAM 2017 were as follows:

- **Week 1: October 2-6 – Theme: Simple Steps to Online Safety.**
- **Week 2: October 9-13 – Theme: Cybersecurity in the Workplace is Everyone's Business**
- **Week 3: October 16-20 – Theme: Today's Predictions for Tomorrow's Internet**
- **Week 4: October 23-27 – Theme: The Internet Wants YOU: Consider a Career in Cybersecurity**
- **Week 5: October 30-31 – Theme: Protecting Critical Infrastructure from Cyber Threats**

Each year during NCSAM, the Multi-State Information Sharing and Analysis Center (MS-ISAC) provides a Cyber Security Toolkit. This resource features educational material designed to raise cyber security awareness through a variety of informative and practical means. This year's toolkit may be found online at https://www.cisecurity.org/ms-isac/ms-isac-toolkit/. The Toolkit has been developed and distributed by the MS-ISAC to all fifty states as well as U.S. Territories, and it can be widely shared across government, businesses, schools and citizens. Additional cybersecurity resources are available at the following sites:

- **DHS Stop.Think.Connect:** https://www.dhs.gov/stopthinkconnect
- **StaySafeOnline:** https://staysafeonline.org/ncsam/
- **NC Cybersecurity Awareness Site:** https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

2017 Cyber Awareness Symposium

On October 19-20, the Enterprise Security and Risk Management Office (ESRMO) hosted a two-day event in support of NCSAM. The event was open to all state and local government employees and was well attended. The event featured several presentations on cybersecurity including Cyber Threat Insights from Dell Secureworks, Leveraging Threat Intelligence by McAfee, Cyber Threats and Information Sharing by the Federal Bureau of Investgation (FBI) Cyber Division, Incident Response and Reporting by the ESRMO, and a panel discussion featuring several agency Chief Information Security Officers (CISO). This year's event was also the first one to provide a second day of hands-on workshops featuring Threat Hunting and QRadar SIEM. Some of the presentations from the event are available on the NC Cybersecurity Awareness site at https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness.

IBM Security

McAfee
Together is power.

The Rural Center
EST. 1987

Secureworks

According to a study by the Center for Cyber Safety and Education, by 2022, there will be a shortage of 1.8 million information security workers. It is critical that people today enter the workforce to fill the vast number of available cybersecurity positions. Week 4 of NCSAM encouraged people to explore careers in cybersecurity. Right on the heels of NCSAM is National Cybersecurity Career Awareness Week which will be **November 13-18, 2017**. This awareness week is promoted by the National Initiative for Cybersecurity (NICE) and will also focus on educating and engaging all age groups to pursue careers in cybersecurity. During the week, people will learn how cybersecurity plays a vital role in their lives and how building a national cybersecurity workforce enhances national security and promotes economic prosperity. For more information about National Cybersecurity Career Awareness Week, please visit https://nist.gov/nice/nccaw, or view the flyer that is attached to the end of this newsletter.

Don't forget, there are other **monthly newsletters** available to you that contain a wealth of information! The following are the various cybersecurity newsletters the ESRMO distributes each month. These newsletters contain information we hope you find beneficial.

- **SECURITYsense Newsletter:** A licensed monthly newsletter that contains several articles involving current cybersecurity issues.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/SECURITYsense

Disclaimer: The SECURITYsense newsletter is a licensed product of the National Security Institute, Inc. (NSI) and is protected by the United States copyright laws. Distribution via an open Internet site (available to anyone with Internet access), Extranet, or other public access network is strictly prohibited.

- **Security Tips Newsletter:** A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month is on ***National Cyber Security Awareness Month 2017***.

https://www.cisecurity.org/resources/newsletter

- **SANS OUCH! Newsletter:** A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is about ***Helping Others Secure Themselves.***

http://securingthehuman.sans.org/resources/newsletters/ouch/2017

Did you know that The SANS Institute also provides *free* awareness videos and webcasts? The SANS **Video of the Month** may be accessed at https://securingthehuman.sans.org/resources/votm.

Also, The SANS Institute offers **free webcasts** on a variety of topics that may be accessed at https://www.sans.org/webcasts/upcoming.

The following training opportunities will be available through the statewide **Learning Management System (LMS)**. These courses are designed to meet the 2017 annual cyber awareness training requirement for State employees.

- **October** – *Public Wi-Fi: Be Careful Out There*
- **December** – *Office Security: Keeping Your Office Secure*

If you have questions about the training schedule or the training content, please contact Maria Thompson, State Chief Risk Officer, at maria.s.thompson@nc.gov or at (919) 754-6578.

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at no cost to government staff, including contractors. With 60+ courses at varying levels of proficiency – from beginners to advanced – all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated on a rolling basis.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ Over **60+** available courses of varying proficiency – beginner to advanced
- ✓ Self-paced
- ✓ Many popular certification courses including:
  - Network +
  - Security +
  - Certified Information Systems Professional (CISSP)
  - Windows Operating System Security
  - Certified Ethical Hacker (CEH)
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework
- ✓ Individuals can take courses to build the required knowledge, skills, and abilities in the cybersecurity field
- ✓ Taught by experienced cybersecurity subject matter experts

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

Upcoming Events…

- ➢ **November 10–15** – 65th Annual International Association of Emergency Managers Conference. More info is at https://iaemconference.info/2017/
- ➢ **November 13-18, 2017** – National Cybersecurity Career Awareness Week. More info is at https://nist.gov/nice/nccaw
- ➢ **November 1-30, 2017** - National Critical Infrastructure & Resilience Month (CISR). More info is at https://www.dhs.gov/cisr-month

---

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies in order to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.

The National Cybersecurity Career Awareness Week, brought to you by the National Initiative for Cybersecurity (NICE), is a week-long celebration focused on increasing awareness about careers in cybersecurity and how building a national cybersecurity workforce enhances America's security and economic prosperity. NICE brings to the forefront information of local, regional, and national interest to inspire, educate and engage citizens to pique their interest in cybersecurity careers. National Cybersecurity Career Awareness Week takes place during November's National Career Development Month, and each day of the week-long celebration provides for an opportunity to learn about the contributions, innovations, and opportunities that can be found by choosing a career in cybersecurity.

Objectives

- Create excitement around increasing public awareness and engagement in building a strong cybersecurity workforce.
- Emphasize the demand and opportunities in the field of cybersecurity.
- Increase awareness around the multiple career options within the field of cybersecurity.
- Highlight the numerous pathways to enter the cybersecurity career field.
- Showcase programs that increase participation of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce.
- Advance the NICE Strategic Plan objective to inspire cybersecurity career awareness with students.

The 2017 events have been organized around the four prongs of the K-12 Cybersecurity Education Implementation Plan*, however, we encourage all stakeholders to engage in the week-long celebration.*

Weekly Events

Day 1: November 13, 2017 – Kickoff Event: Career Opportunities in Cybersecurity

Day 2: November 14, 2017 – Increasing Career Awareness of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce.

Day 3: November 15, 2017 – Webinar highlighting Innovative Educational Approaches: Nontraditional Pathways of Apprenticeship and Cooperative Education

Day 4: November 16, 2017 – Infusing Cybersecurity Across the Education Portfolio

Day 5: November 17, 2017 – Identifying Academic and Career Pathways

Day 6: November 18, 2017 – Increase Career Awareness through Informal Activities

Day 1: November 13, 2017 – Kickoff Event: Career Opportunities in Cybersecurity
K12 Implementation Plan: *Increase Career Awareness: Increase and Sustain Youth and Public Engagement in Cybersecurity Activities. (a) Establish a cybersecurity career awareness campaign targeting educators, students, parents, administrators, and counselors.*

The Kickoff will be a day devoted to increasing public awareness and engagement about the cybersecurity workforce. Day 1 will celebrate the inaugural cybersecurity career awareness campaign targeting educators, students, parents, administrators, and counselors.

Day 2: November 14, 2017 – Increase Career Awareness of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce.
K12 Implementation Plan Aim: *Increase Career Awareness: Increase and Sustain Youth and Public Engagement in Cybersecurity Activities. (c) Increase the appeal of the cybersecurity profession to a diverse audience.*

Day 2 will feature activities and programs that target underrepresented groups.

Day 3: November 15, 2017 – Webinar Event: Nontraditional Pathways of Apprenticeship and Cooperative Education. K12 Implementation Plan: *Stimulate Innovative Educational Approaches.*

To connect with this week also being National Apprenticeship Week, Day 3 will host a webinar that combines these two important events.

Day 4: November 16, 2017 – Infusing Cybersecurity Across the Education Portfolio
K12 Implementation Plan: *Stimulate Innovative Educational Approaches: Design Cybersecurity Education for the future STEM and Cybersecurity Workforce].*

Day 4 will highlight local, state, regional, and national efforts that have successfully integrated cybersecurity into the formal classroom curriculum. Showcased efforts may include CSTA's cybersecurity components within the refresh of the computer science standards, NICERC curriculum and professional development, South Carolina and Virginia's cybersecurity standards/content, California and Georgia's model curricula, etc. Other resources will be shared on the NICE website.

Day 5: November 17, 2017 –Identify Academic and Career Pathways
K12 Implementation Plan: *Identify Academic and Career Pathways: Increase the number of youth pursuing a cybersecurity or cybersecurity related degree, certificate, or job.*

Day 5 with spotlight the growing interest in Early College Programs and P-Tech.

Day 6: November 18, 2017 – Increasing Cybersecurity Career Awareness through Informal Activities
K12 Implementation Plan Aim: *Increase Career Awareness: Increase and Sustain Youth and Public Engagement in Cybersecurity Activities. (b) Develop informal/co-curricular experiences (e.g., competitions, camps, clubs, boy/girl scouts, etc.) for youth that excite them about careers in cybersecurity and introduce them to the corresponding academic pathways.*

Day 6 will spotlight activities that excite youth about careers in cybersecurity. A wide variety of efforts will be showcased including, but not limited to: NSA Day of Cyber, GenCyber camps, other local and state based camps, competitions, Girl/Boy Scouts, 4H, and Robotics. A tool kit and other resources is made available for use by teachers in the classroom, by guidance counselors at career fairs, and by parents to help their children plan their future. We will encourage industry and government partners to visit schools to promote cybersecurity careers.