North Carolina
Cybersecurity
Awareness Month
(NCSAM)

Maria S. Thompson
State Chief Risk Officer
WHY CYBERSECURITY AWARENESS IS CRITICAL

https://www.youtube.com/watch?v=Ru0y5rCETqc&feature=youtu.be
AGENDA

- 0900 – 09:45  Opening remarks – Maria Thompson, State Risk Officer
- 09:45 – 10:45  Cyber Threats & Vulnerabilities - Chris Hallenbeck, Regional CISO - Tanium
- 10:45 – 11:00  [BREAK]
- 11:00 – 12:00  Cybersecurity & You - Jim Boyles – IBM Cybersecurity Architect
- 12:00 – 01:15  [LUNCH]
- 01:15 – 02:15  Insider Threat Mitigation Best Practices - Jeremy Manning – Secureworks Counter Threat Unit
- 02:15 – 02:50  Statewide Cyber Incident/Threat Briefing – Albert Moore, DIT Threat Intel Lead
- 02:50 - 03:00  [BREAK]
- 03:00 – 03:45  Lessons Learned After Hurricane Florence - Debora Chance – DIT ESRMO Business Continuity
- 03:45 – 04:45  O365 Security Solutions & Best Practices – Ken Nuebler, DIT
- 04:45 – 05:00  CLOSING REMARKS
Today’s cyber risks are increasing. New technologies bring greater capabilities at a trade off. Convergence of traditional systems and IT networks creates more risks to be mindful of.

- Hackers Breach Web Hosting Provider for the Second Time in the Past Year
- Arrest of Top Chinese Intelligence Officer Sparks Fears of New Chinese Hacking Efforts
- New Threat Group Conducts Malwareless Cyber Espionage
- New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom
- GAO Audit Reveals Cyber Vulnerabilities in U.S. Weapons Systems
Current State of Cyber Threat Landscape

...You are only as strong as the weakest link!

- Between 50 – 70% of incoming emails are identified as Phishing, SPAM or Virus
- The past couple of years, local counties have reported an uptick in ransomware
- There is a reported 133% increase in data breaches reported by first half of 2018 in comparison to previous year
- The use of Internet of Things increase daily...along with their associated risks
- Business owners continue to accept risks blindly...
Strategic Plans & Best Practices

Effective cybersecurity practices, governance policies and risk assessment methods. Standardized approach ensures interoperability and secure operations.

- Implemented the NIST RMF
- Continuous Monitoring – 24 X 7 X 365 cyber monitoring and incident response
- Develop, implement an test Incident Response Plans
- Conduct cyber resiliency exercises
- 918A ala Carte security convenience contract
  - Identify new and evolving risks
  - Assess and prioritize risks
  - Develop and prioritize mitigation strategies based on cost-benefit analysis and other factors
  - Evaluate the impacts of mitigation implementation
Strategic Plans & Best Practices

- Vendor Risk Management!!!!
- Cyber Education and Awareness campaign
- Continuity of Operations and Disaster Recovery
- DevSecOps – For the Developer in YOU!
- Implement Insider Threat Program
- Protection and visibility for Cloud services
- Cyber Workforce Development
Free Cybersecurity Training Resources

Federal Virtual Training Environment (FedVTE)
- Course proficiency ranges from beginner to advanced levels. Several courses align with a variety of IT certifications such as Certified Information Systems Security Professional (CISSP), CISA, CEH, Pen Testing etc.
  ✓ https://niccs.us-cert.gov/training/fedvte

- National Initiative for Cybersecurity Careers and Studies
  ✓ https://niccs.us-cert.gov/formal-education