Monthly Cybersecurity Newsletter
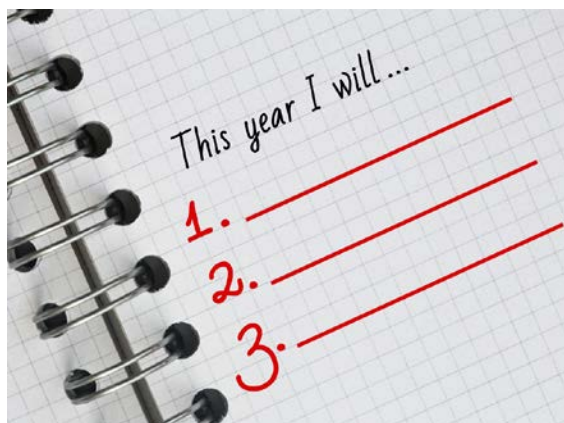
Enterprise Security and Risk Management Office (ESRMO)

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

Happy New Year! What will you resolve to do?

The ESRMO would like to share this monthly newsletter with information we hope you find beneficial. As we say farewell to the year 2016 and welcome a new year 2017, it is a good time to remind ourselves of **our shared responsibility** to keep the State of NC safe from cyber threats. Some resolutions we could make for this year are as follows: to use strong passwords for all systems; to recognize suspicious email and avoid phishing attempts by not clicking on links in them; to not download or install unauthorized software; to avoid connecting to a public Wi-Fi; and to use secure methods to store and transmit sensitive State data. Together, we can help make the State of NC a safer place to conduct business online.

The following are the various cybersecurity newsletters we distribute that contain information we hope you find beneficial.

SECURITYsense Newsletter: A licensed monthly newsletter that contains several articles that are usually relevant to 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) that is usually on a single topic intended to increase cybersecurity awareness.

http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-tips-newsletters

SANS OUCH! Newsletter: A free monthly information security awareness newsletter provided by The SANS Institute that is usually on a single topic.

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

We would like to share the following information about some upcoming E-commerce/PCI Data Security Standards educational opportunities that the Office of the State Controller (OSC) is promoting with the help of Coalfire:

- February 14 at 10:00am – Continuous Compliance: Implementing a Business-As-Usual Approach to PCI Compliance
- April 11 at 10:00am – What is a Pen Test and How to Pick a Good Pen Tester?
- June 20 at 10:00am – What is P2PE Encryption?
- August 15 at 10:00am – What is a Physical Security Assessment and Benefits?
- October 24 at 10:00am: Implementing an Effective Employee Security Training Program
- December 5 at 10:00am - *TBD*

Each webinar will last approximately 1 hour. Additional information for each of the webinars, along with a registration link will be distributed a few weeks prior to the scheduled event.

OSC will also be hosting a 2017 E-Commerce Conference at the NCSU McKimmon Center on April 19, 2017. Additional information about this event, including topics, cost, registration process, etc., will be sent out in early March.

With the new year, we have plenty of new training opportunities. The following is the 2017 Cyber Awareness Schedule that is provided through the statewide Learning Management System (LMS):

- February - Incident Reporting: Recognize and Report Security Incidents
- April - Information Protection: Protecting Information
- June - Computer Security: Don't let your Computer's Defenses Down
- August - Mobile Security: Mobile Devices – The Future is Now
- October - Public WiFi: Be Careful Out There
- December - Office Security: Keeping Your Office Secure

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

We would like to remind you all of the Corporate Executive Board (CEB) Membership – Information Risk Leadership resource that is available. This is an ESRMO funded license and is free to all agencies. Through this membership, all State employees have unlimited access to CEB's proprietary quantitative databases, best practices case studies, on-demand customized research, interactive member networking events, online benchmarking data, issue-specific resource centers, and diagnostic tools and templates. CEB recently announced an agreement to be acquired by Gartner, a leading information technology research and advisory company.

Your CEB username and password will grant you full access to all of CEB's councils. To gain access to this resource, follow the steps below to set up your Username/Password:

- Visit the partnership website listed below:
  - Information Risk Leadership Council – irec.executiveboard.com
  - Enterprise Architecture Leadership Council – eaec.executiveboard.com
- Enter your contact information as requested, using "State of North Carolina" as your Organization.
- A link to confirm your username (which will be your @nc.gov email) and set password will be emailed to you shortly.

Lastly, we encourage all security professionals to send us topics that will be of value to other agencies in order to foster better information sharing and awareness. If you have a suggestion for a topic to share with others and would like for us to consider including it in a future newsletter, please send it to security@its.nc.gov.

Resources to Remember

Cybersecurity and Risk Management Site:
http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management

ESRMO SharePoint Site:
https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/default.aspx

State of NC Cybersecurity Incident Reporting Site:
https://it.nc.gov/cybersecurity-situation-report

Homeland Security Information Network (HSIN) Site:
https://hsin.dhs.gov