Monthly Cybersecurity Newsletter

March 2017 Issue

Information Technology

Enterprise Security and Risk Management Office (ESRMO)

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

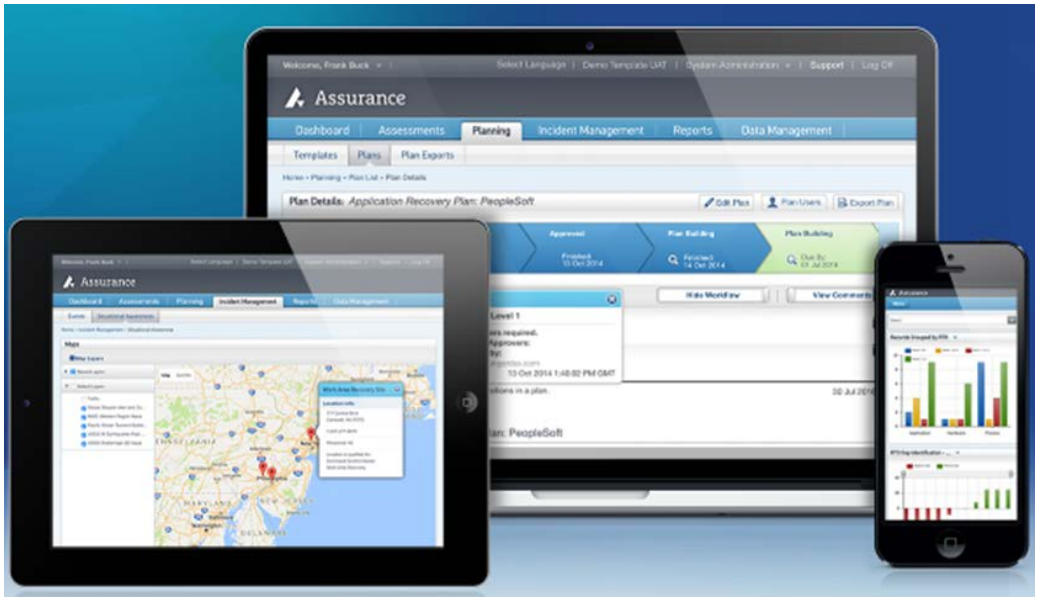
---

Transitioning from LDRPS to AssuranceCM

New to the State of North Carolina's technology department is the AssuranceCM application, provided by Sungard Availability Services (AS). The State was utilizing a different Sungard product, known as LDRPS, for business continuity and disaster recovery plans. Sungard AS decided to launch a new solution, AssuranceCM, to provide some new Business Continuity/Disaster Recovery (BC/DR) programs. The State evaluated the new system, as well as others in the marketplace, and decided to transition to AssuranceCM. Some of the new key features include automated scheduled data imports, Business Impact Analysis and Incident Management modules, integration with an emergency notification service, mobile capability, and an intuitive user interface. DIT began transitioning to the new solution in late December 2016 and will complete the transition by mid-year 2017.

The transition process is a vital action for ensuring the State's data and plans are seamlessly brought over into the new system. The ESRMO is working very closely with a Sungard AS Analyst to transfer all of the critical elements over and assist with rebuilding items such as templates, reports, and security based on the necessary requirements. AssuranceCM will give a much more efficient approach to building BC/DR Plans and also provide incident and testing capabilities.

The images on the right are some screen shots from the AssuranceCM solution.



The Day 9-1-1 *Almost* Died!

In October 2016, the Maricopa County Sheriff's Office in Phoenix Arizona faced a crisis. The emergency 911 system for the entire Phoenix metro area experienced a serious disruption due to a cyberattack. An 18-year old discovered a vulnerability that allowed him to use JavaScript remotely and cause Apple iOS devices to make phone calls without the end user's intervention. The individual created code that caused iPhones to dial the emergency number 911, in an apparent attempt to claim money from Apple for discovering the bug. He put the code on his own webserver, and shared the link via Twitter and his YouTube channel. Authorities believe that one tweeted link was clicked 117,502 times, each click triggering a 911 call. The emergency 911 system was simply overwhelmed by the attack. This type of exploit reveals the obvious need to be leery of clicking on links, even from our mobile devices, as well as the need to make all types of infrastructure more resilient to cyberattack. For more information about this topic, see https://9to5mac.com/2017/03/06/911-ios-exploit/.

Don't forget the other monthly newsletters we provide! The following are the various cybersecurity newsletters the ESRMO distributes each month. These newsletters contain a variety of information that 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

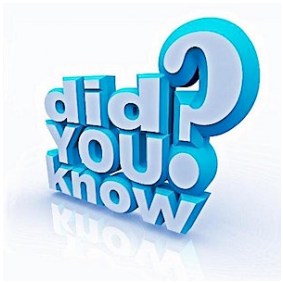
Disclaimer: The SECURITYsense newsletter is a licensed product of the National Security Institute, Inc. (NSI) and is protected by the United States copyright laws. Distribution via an open Internet site (available to anyone with Internet access), Extranet, or other public access network is strictly prohibited.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's topic is titled ***Common IT Wisdom That Keeps You Secure.***

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. This month's topic is titled ***Securely Using Mobile Apps***.

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



Did you know that The SANS Institute also provides free awareness videos? The Video of the Month for this month is on "Social Engineering". In this short video, they explain what social engineering is, provide two different examples of social engineering, and tell you how you can easily spot such attacks. Check it out!

https://securingthehuman.sans.org/resources/votm

When A DoubleAgent Attacks

A newly found zero-day attack is being called DoubleAgent because it turns your antivirus software into a malicious agent. The attack makes you think your antivirus protects you while it actually attacks you, such as encrypting files for ransom, exfiltrating data, or formatting your hard drives. Based on a 15-year-old feature called the Microsoft Application Verifier Provider that is in all Microsoft Windows versions, DoubleAgent gives the attacker the ability to inject any dynamic link library (DLL) into any application process. The code injection occurs early during the process boot, giving the attacker full control over the process and no way for the process to protect itself. It even persists after reboots, updates, reinstalls and patch installations. Most of the current security products on the market are susceptible to the DoubleAgent attack. Software vendors were notified more than 90 days ago, which gave them time to fix the issue. As a mitigation, researchers say the simplest fix for antivirus vendors is to switch from Application Verifier to a newer architecture called Protected Processes.

As a reminder, the NC Office of the State Controller (OSC) is promoting the following E-commerce/PCI Data Security Standards educational opportunities with the help of Coalfire:

- 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. More information about this event, including topics, cost, registration process, etc., may be found online at http://osc.nc.gov/ecommerce2017.

The ESRMO would like to also remind you of the new training opportunities we have through the statewide Learning Management System (LMS). The following is a list of the 2017 Cyber Awareness training modules that are provided through LMS.

- 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 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.

Don’t forget to check out the following resources:

Department of Information Technology (DIT) Site:
https://it.nc.gov/

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

Cybersecurity Awareness Page:
https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

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

Do you have something to share? Is there a topic you think we should cover in a future newsletter? 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.
