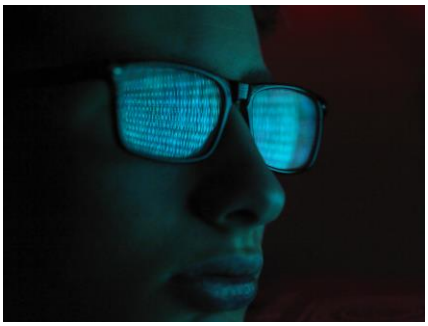
Monthly Cybersecurity Newsletter

April 2021 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

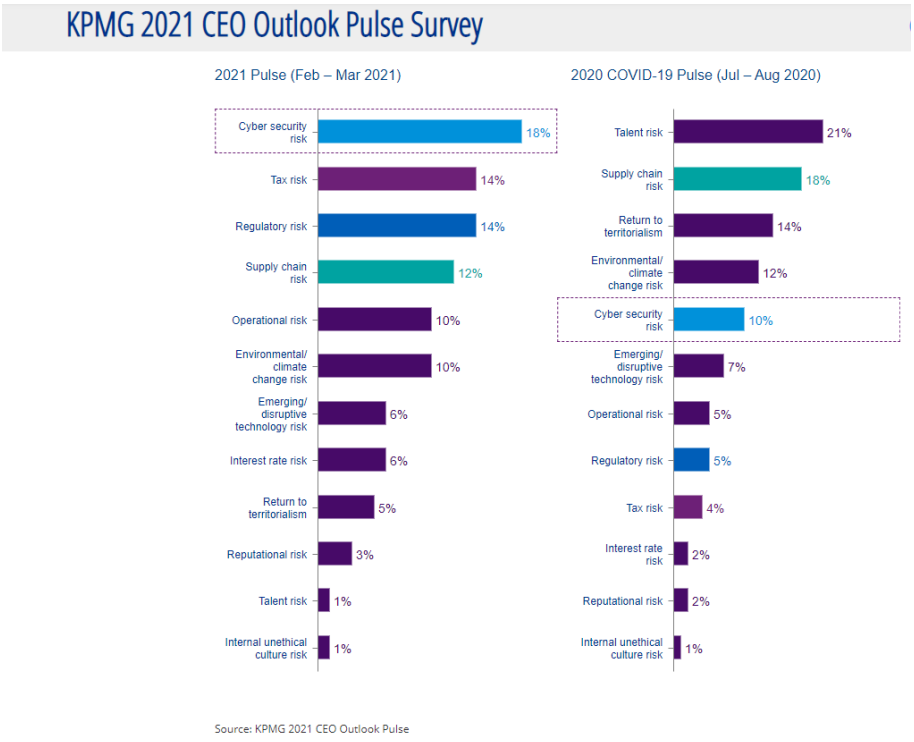
From the Desk of the State Chief Risk Officer – Maria Thompson



Cybersecurity Risk Is Now The Leading Threat To Growth!

KPMG in the UK, a leading provider of tax, audit and advisory services, just released their CEO 2021 Outlook Pulse Survey. This annual survey asked 500 CEOs from around the world to provide their three-year outlook on the economic and business landscape, as well as the ongoing COVID-19 pandemic. The respondents to the survey represented eleven key industry sectors (asset management, automotive, banking, consumer and retail, energy, infrastructure, insurance, life sciences, manufacturing, technology, and telecommunications) from eleven nations.

With a year of adapting to the pandemic, these CEOs are planning what a return to "normal" will look like. Nearly half (45 percent) expect normality to resume in 2022, with only one-third (31 percent) anticipating a return to normal in 2021. Significantly, 24 percent of leaders say that their business has ***changed forever***. When asked, which of the following risks poses the greatest threat to your organization's growth over the next three years, cybersecurity was the ***number one response***. This view has evolved since last year where cybersecurity risk was in ***fifth place***. See chart for results.



One result of this outlook is that CEOs are shifting their primarily focus to cybersecurity issues and digital connectivity with their customers. They plan to spend more money on digital technologies than the previous year, with 52 percent prioritizing data security measures.

For the full article with the complete survey results, visit here.

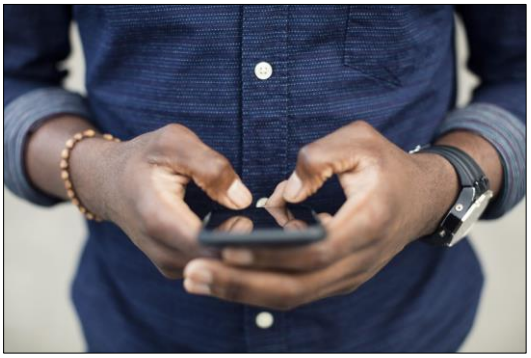
NSA Releases Guidance on Zero Trust Security Model

Ronald Regan popularized the Russian proverb "Trust, but verify" during his presidency and used it frequently when discussing U.S. relations with the former Soviet Union. The National Security Agency (NSA) is now saying "**Never trust, always verify**." The NSA has released Cybersecurity Information Sheet: Embracing a Zero Trust Security Model, which provides information about, and recommendations for, implementing Zero Trust within networks.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside an organization's network and systems. The Zero Trust security model eliminates implicit trust in any one element, device, or service on the network. Instead, it requires full visibility of all activity across all layers from endpoints and the network to enable the analysis of data that can detect suspicious activity. This model ***assumes*** breaches are inevitable or have already occurred.

The Cybersecurity & Infrastructure Security Agency (CISA) encourages administrators and organizations to review NSA's guidance on Embracing a Zero Trust Security Model to help secure sensitive data, systems, and services.

Mobile Device Management Policy Released



Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals. Just about everyone has a mobile computing device and we find it hard to be without one. While mobile devices are important, they can also represent a significant risk to the security of the network and data if appropriate security controls and procedures are not implemented. Furthermore, if not carefully managed, mobile devices can be a conduit for unauthorized access to the network, which can subsequently lead to data leakage, breaches, and network compromise.

The Enterprise Security and Risk Management Office (ESRMO) is pleased to announce a **Mobile Device Management Policy** has been released. The new policy provides the requirements for approved mobile devices to operate and access the State network and systems to conduct State business. The policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State. The Mobile Device Management Policy may be found via the link below:

https://it.nc.gov/documents/statewide-policies/mobile-device-management-policy/download

To review other State information security policies and cybersecurity related information, please visit the NC DIT Cybersecurity & Risk Management site.

Assurance^{CM} Production Update!

On the evening of **Friday, April 2nd, 2021**, Castellan Solutions will be updating the Assurance CM US Production environment with the latest release of Assurance CM. The update will take place between the hours of 8 PM – 12 AM (EDT). During this time, your Assurance CM database will be available, however you may experience a service interruption at times.

PCI Webinars by Coalfire

The N.C. Office of the State Controller is pleased to announce that Coalfire, a PCI Compliance Validation Services vendor for the state of North Carolina will be presenting four webinars in 2021. The scheduled dates are as follows:

Date	Topic (tentative)
June 15, 2021	Vulnerability Scanning and Penetration Testing – What is the Difference?
Sept. 7, 2021	Authentication and Access Control – Who Are You?
Dec. 7, 2021	Risk Assessments – Do you Feel Lucky?

All webinars will begin at 10 a.m. EST and will be approximately one hour. Additional details (including registration information) will be sent out in advance of each webinar. For the current list of webinars being provided by the Office of the State Controller, please visit here.

Please Note: The PCI webinar announcements are distributed through the eCommerce listserv. If you are interested in receiving this information directly, please register online. The eCommerce listserv also provides updates for products and services on the Merchant Card and EFT Master Services Agreements, as well as webpage and enrollment form updates and reminders regarding annual PCI Compliance, SAQs and Quarterly Scans.

Join Roger Grimes, KnowBe4's Data-Driven Defense Evangelist to find out how cyberwarfare has evolved and why any organization can be a target. In this webinar, you will learn why these attacks now impact organizations of all sizes and industries, and how you can mitigate the threat of nation-state attacks. For more information and to register for this webinar, click here.

Mobile Devices and Remote Security

Smartphones, tablets, and other devices keep us connected no matter where we go. They also present significant security challenges from both a professional and personal standpoint. Here are a few common threats and tips for how to avoid them:

PUBLIC WIFI	Public WiFi poses a major threat to privacy. You can mitigate that threat by using a virtual private network (VPN)—software that encrypts your connection and prevents others from stealing your data. But even with a VPN, it's still best to avoid accessing highly sensitive information when connected to public networks.
UNPATCHED VULNERABILITIES	Out-of-date devices and software leave doors open for cybercriminals who use known vulnerabilities to install malware or steal data. Enable automatic updates wherever possible, so you'll never miss a critical security patch.
MALICIOUS APPS	Scammers create malicious apps—often impersonating legitimate apps—to invade privacy. Before downloading or installing any software, research the developers and confirm they are legitimate. Once installed, carefully review the permissions and security settings to ensure the app isn't collecting more data than necessary. Always check our organization's current policies before installing any apps or software on work-issued devices.
PUBLIC CHARGING STATIONS	Many public places now offer free USB charging stations. Unfortunately, they represent yet another way for cybercriminals to spread malware via an attack called "juice jacking," where they compromise your device via a USB connection. Only use the USB devices and chargers that belong to you.
SMISHING	With messaging apps exploding in popularity, it's no surprise that smishing—phishing via text message—attacks continue to rise. Never click on links or respond to text messages from unknown users, especially those who use threatening or urgent language.
SHOULDER SURFING AND DEVICE THEFT	Utilize situational awareness! When you're in public areas or traveling, make sure no one can see your screen. Keep an eye on your belongings, and never leave desirable items in plain sight. Use discretion when discussing or accessing anything that might be deemed confidential. To avoid losing any devices or other important items, perform an inventory check before exiting public transportation, checking out of hotels, and deboarding airplanes.

Key Takeaways:

- Always use a virtual private network while connected to public WiFi.
- Stay alert for phishing attacks that target you via text message.
- Keep devices and software up to date and allow automatic updates when possible.

Stay Safe While Working from Home

Working remotely has its benefits, ***but*** it comes with added responsibility. Click here for tips on how to stay secure while working from home.

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4.
***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2021

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/security-awareness-training/ouch-newsletter

April 7: SANS Webinar: *Taking a behavioral approach to security- how to stay one step ahead of your adversaries*

April 7: KnowBe4 Webinar: Nation-State Hacking 2.0: Why Your Organization is Now at Risk from this Evolving Threat

April 27: SANS Webinar: What SolarWinds Taught Us About Third Party Risk Management

May 10-14: AI Week: Week-long tech festival dedicated to artificial intelligence (AI)

May 17-21: Business Continuity Awareness Week (BCAW)

Also, for a list of upcoming SANS webcasts, visit here.

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember… Stop. Think. Connect.*

***Disclaimer**: Vendors, references, and links in this newsletter are for informational purposes only and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*