

September FY2017 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

*Happy New (fiscal) Year!*

## October is Coming! October is Coming!

Ok, so it's not exactly like revolutionary times, and I may not be Paul Revere, but it is that time of year again! As October, National Cybersecurity Awareness Month, approaches, now is a good time to put on the security evangelist hat and try and prevent one person from clicking on that one bad email that will completely shut down your network.

When thinking about the security program at your agency, awareness should be ingrained into every division, project and employee and practiced regularly throughout the year. But Cybersecurity Awareness Month is a great reason to really focus on helping your customers become more aware and vigilant regarding information security practices and have a little fun with security awareness.

You may be wondering how to create a full campaign around security awareness. Here are a few ideas to get the creative wheels turning:

- **Clearly define one or two topics upon which you would like to focus.** Concentrate on social engineering, phishing, Internet or email usage, etc. Narrowing the spotlight and determining what type of results you'd like to see can help ensure you deliver a clear message and foster a user community focused on security awareness.
- **Come up with a fun theme.** Play off of current events such as the summer Olympics or Halloween or go in a new creative direction. A good theme can spark ideas for different types of events and generate more interest in the campaign. A few years ago, the CDC used a zombie theme to spread awareness about preparedness for emergencies that was effective and fun.
- **Plan for a few different kinds of events.** This could include games that introduce common security terms/best practices, learn-at-lunch sessions and pop-up messages on the user's login screen with a security topic.
- **Use resources provided.** There are resources available if you don't know where to start. Every year, the MS-ISAC (co-hosted with the Department of Homeland Security) publishes a toolkit with resources. This toolkit includes posters, calendars, social media sample posts and weekly themes. If you would like these materials, contact [DIRSecurity@dir.texas.gov](mailto:DIRSecurity@dir.texas.gov). The materials are still getting prepared, and should be ready later this month for downloading. [Check the MS-ISAC Website for more information.](#)
- **Look to your peers for brainstorming ideas.** The monthly ISWG meetings are a great way to exchange ideas, or look for assistance from other ISOs. The Security-Officer and Security group mail lists are other good ways to exchange information.
- **Let DIR help.** DIR will be hosting a few events throughout the month. These will be one-two hour sessions that will be open to all agencies. More information about these sessions will be sent out soon – so be on the lookout!

## CONTENTS

### Monthly Article

October is Coming! P.1

### Program Updates

InfoSec Academy P.2

NSOC Update P.3

Agency Security Plan P.3

SANS Securing the Human (STH) Update P.3

### Interest Articles

Happy Catching P.4

Biometrics – The Inherence Factor of Authentication P.5-6

### Our State ISO

### Spotlight

Jeff Barrington P.7

Events p.8

# InfoSec Academy Update

The Texas InfoSec Academy is off to a great start! Approximately 40 people have already completed the Texas Security Policy & Assurance class, enabling them to enroll in certification prep and a variety of other courses. For information on the courses available, prerequisites, who is eligible and number of courses by agency size, please see the chart below:

Course	Pre-requisite	Eligible Participants
<b>Texas Security Policy &amp; Assurance</b> offered in an instructor led class and also in an online anytime format	None	All security staff from state agencies & IHEs.
<b><u>Online Live (OLL) Certification Prep Courses this includes:</u></b> Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM) Certified in Risk and Information Systems Control (CRISC) CompTIA Security+ Certified Ethical Hacker	Texas Security Policy & Assurance	CISOs & ISOs from state agencies & IHEs and security staff if approved by CISO/ISO.  <b><u>Number of Courses Limit each FY:</u></b> Small Agency: 1 Medium Agency: 3 Large Agency: 5  Medium or large agencies can distribute these classes among one or more people on the security team.
<b><u>Online Anytime (OLA) Libraries this includes access to the following 3 libraries:</u></b> Business Skills Cybersecurity (including some certification prep courses) IT Course	Texas Security Policy & Assurance	All security staff from state agencies & IHEs with approval from the CISO/ISO.  <b><u>Participant Limit Per FY:</u></b> Small Agency: 1 Medium Agency: 3 Large Agency: 5  Participants can be the same or different from those taking OLL courses.
Courses available under the "Search All Courses" buttons.	Texas Security Policy & Assurance	Any security staff is eligible to submit a registration, but these registrations must be approved by DIR.

**Upcoming instructor led Texas Security Policy & Assurance classes are scheduled from 8:00 to 4:00 on the following days:**

September 16, 2016

November 21, 2016

January 16, 2017

Instruction will occur at the New Horizons Austin location at 300 E Highland Mall Blvd, Suite 100, Austin, TX 78752. An online anytime version of the Texas Security Policy and Assurance course is also available. If you would like to sign up, [VISIT THE INFOSEC ACADEMY](#) website. If you have any questions about the InfoSec Academy send an email to [infosecacademy@dir.texas.gov](mailto:infosecacademy@dir.texas.gov).

# NSOC Update

---

An email was sent out to all ISO's on 8/16/16 about a hardware issue that we had on our IPS at the NSOC and I wanted to provide a little more detail. The DIR Network Security Operations Center had a hardware failure on one of its enterprise IPS devices Sunday, Aug. 14 around 2:48 p.m. Traffic was moved to the backup IPS at approximately 5:45 p.m. the same day. This resulted in approximately three hours when traffic was not blocked by the NSOC's IPS. At 4:05 p.m. Monday, Aug. 15, the backup IPS also had hardware failure.

The issue resulted in almost 16 hours of time when traffic was not being blocked. The system was rebooted and services were temporarily restored at 7:51 a.m. The system then failed again at 9:19 a.m. until 10:45 causing another hour and a half window where the IPS wasn't blocking. At 10:45 a.m. the backup enterprise IPS was restored and inspecting and blocking capabilities were restored. The replacement for the enterprise IPS was received and prepared for installation by 1:12 p.m. on Tuesday the 16th. Traffic was then switched to the replacement IPS at 5:30 pm on the 16th. This enables the NSOC to provide both primary and backup blocking and inspecting. The replacement for the backup enterprise IPS has been received and configured which allows us to ensure we maintain primary and backup IPS capabilities. During this time of enterprise IPS failure, all remaining tools in the NSOC security stack were up and monitoring for malicious traffic. These tools include two diverse intrusion detection systems, a malware detection system and a network forensics tool. NSOC analysts are reviewing the logs of the working tools for signs of anomalies. NSOC analysts will continue to alert agencies to any abnormal findings. Currently a TAC case is opened with a vendor for a true forensics and Root Cause Analysis (RCA). However, the current assessment is that this was a hardware failure. NSOC is reviewing our architecture and considering options for adding in other security devices. These options include but are not limited to, high availability mode, multiple inline devices, replacing existing vendor solution and combinations of previous options.

Should you have any question, please send an email to [security-alerts@dir.texas.gov](mailto:security-alerts@dir.texas.gov) or call us at (888) 839.6762.

## CAUTION: Due Date Ahead

---

On October 15, your SPT is due.

That's right! Each agency and higher education institution is required to submit their security plan template to DIR by October 15 of even numbered years. The data from 2014 is loaded into the SPECTRIM portal so that you can use that as your foundation for this year's plan. [You can find information about the SPT on the DIR website here.](#) You can find information about the SPECTRIM portal [here](#).

## SANS Securing the Human (STH) Update

---

DIR's contract with SANS Securing the Human (STH) is expiring at the end of October and we are working on the contract renewal but we are not expecting any breaks in service. The platform for STH has changed & enhancements have been added. These changes will most likely necessitate account administrators to reload users. In preparation for the update, we ask participating organizations to work on having as much of the current training completed as possible. Transcripts and training records will be retained. As we move closer to renewal, more information will be available & we will keep you posted.

# Happy Catching

---

There is no doubt that Niantic Lab's Pokémon GO is a phenomenal success. It is hard not to hear about the hot new application any time you visit your favorite news website, magazine or watch TV. Along with the Real World Gaming Platform, there are other aspects of the game that could be a cause of concern.

Pokémon GO is a game where the objective is to capture different kinds of animals (called Pokémon). The game features Pokéstops (located at real, physical locations) which allow players to restock supplies to be more successful in the game. Walking around parks and popular landmarks hunting these virtual animals encourages users to get exercise and meet others playing the game.

Although Pokémon GO is a current fad for kids (and some adults), there are some inherent risks that accompany this revolutionary game. As with any smart phone app, users must be aware of what data is being accessed as a consequence of having that application. Pokémon GO, like most "free" applications, recoups their development costs by gathering valuable geolocation data and offering in-app purchases. In addition to the data collected by Niantic Labs, there are two main concerns with Pokémon GO that any player, player parent or casual observer needs to know.

First, many smart phone users are already oblivious to the real world around them, but this problem is amplified by this application. Although the game designers have built in beneficial features to promote a healthy lifestyle and physical activity, this can create a danger to pedestrians and motorists. Physical awareness must be maintained by a player so they don't walk into a manhole, light post or worse. Drivers and cyclists must also be more aware as a new breed of distracted people move in search of Pikachu.

Second, as merchants see Pokémon GO as a business opportunity, criminals are also looking for ways to capitalize on the growing number of Poké players. Lack of awareness by the players can give a thief the opportunity they need to strike against the distracted player. A more nefarious way the game can aid a criminal is to use a Pokéstop to lure potential victims to a place they would not visit under normal circumstances. Niantic Labs has become aware of this risk and implemented a tool to remove Pokéstops that are on private property or in a dangerous geophysical area.

The jury is still out as to whether or not Pokémon GO is here to stay. Only time will tell. So have fun out there – just be careful doing so. Happy catching.

## Biometrics – The Inherence Factor of Authentication

---

Authentication is imperative to ensure confidentiality is not compromised when handling data. Of all the authentication factors (something you know, something you have, something you are), the most difficult authentication method to falsify is Something You Are, also known as biometrics. This includes anything from physical (fingerprints, retinal scans and facial recognition) to behavioral (signature geometry and voice identification) inherence of a person.

This type of authentication bordered on the lines of science fiction many years back, when the only times most people would ever see instances of biometrics would be in the movies. Now it's becoming more and more mainstream. We see examples of biometrics at amusement parks when selling annual passes, laptop PCs and USB flash drives with built-in fingerprint scanners, airport security employing iris readers and even public libraries utilizing signature registration. It's a brave new world out there!

A rise in popularity of biometrics also comes a greater interest in comprising this authentication method. It is believed that biometrics is the hardest authentication factor to falsify. In a way, that's still true. Faking a fingerprint is much harder than guessing a poor password. You can easily change a password. Changing your fingerprint is a little harder.

In December 2014, The German defense secretary, Ursula von der Leyen, had her fingerprint copied using high-definition photographs (*one released to the public, from her own office*) and the commercially available software, Verifinger. At the Usenix security conference, in August 2016, security specialists demonstrated how they were able to fool facial recognition software by using 3-D rendered, VR-style facial models based on pictures found through social media. Though faking a system that utilizes biometrics for authentication is hard, it's not impossible.

One way to combat the compromising of biometrics is to use a multimodal system where both multiple, physical and behavioral biometrics are used. It's more difficult to present two convincing inherence factors than one. Another idea is to use text-dependent, voice-based (or speaker) biometric authentication. This type of biometric authentication relies on both the user's physical structure of their vocal tract as well as the behavioral characteristics of the user. A falsifier would have to learn both the emphasis of a phrase and how to distinctively sound like the speaker to circumvent authentication. Of course, a more common approach would be to use multi-factor authentication such as a retinal scanner and keycard or a fingerprint identifier and a passphrase. Keep in mind that no system is ever perfect. However, we can hope to minimize our risk by maximizing their effort.

If you'd like to learn more about biometrics and their role in authentication, visit the articles below.

<http://searchsecurity.techtarget.com/definition/two-factor-authentication>

<https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/>

<https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands>

<http://www.telegraph.co.uk/technology/2016/05/26/biometrics-will-replace-passwords-but-its-a-bad-idea/>

<http://www.biometricsinstitute.org/pages/faq-6.html>

# Information Security Officer Spotlight



**Jeff Barrington**  
Assistant Vice President for IT  
and Information Security Officer  
Texas Tech University

*Founded in 1923, Texas Tech University is a major public research university in Texas with over 36,000 students, offering Baccalaureate through doctoral degrees. Tech is a great place to work! For more information, visit: [www.ttu.edu](http://www.ttu.edu)*

My undergraduate degree is in Information Technology. While working at Texas Tech, I have been completing my MBA at Texas Tech University and plan to graduate in December 2016.

I served in the U.S. Army for eight years as a Staff Sergeant, then Cingular Wireless. I also worked for an IT Services company for several years and came to Texas Tech about six years ago. Through these different companies, I have gained skills in wireless, systems management, network administration, data center management, facilities management as well as customer service and support.

**Tell us how information security has changed since you started in your role.**

In the length of time I have been in this industry, security has changed greatly. In the early years, it was a minor aspect of IT operations and today security is at the forefront of everything we do. All IT professionals should incorporate security in all that they do from system design to programming to access controls.

**Who are your customers, and what is one of the most challenging areas for you?**

Our students, faculty, researchers and staff are our customers. One of the most challenging areas for our team is making sure that our customers are updated with current trends in the area of security and also staying ahead of cyber criminals who are becoming very good at social engineering.

**Top 3 life highlights:**

1. The births of my 4 children
2. My marriage
3. My current role as Assistant Vice President for IT and Information Security Officer at Texas Tech.

**Tell us about your most proud accomplishment.**

Being the first college graduate in my family.

**What do you like best of your job?**

The great team of people I have the honor of working with.

**Least favorite food?**

Brussel Sprouts

**People would be surprised to know that you...**

Were a Military Police Officer in the Army.

**If you could interview one person (dead or alive) who would it be?**

Jesus Christ

**What are your hobbies?**

Spending time with my family, golfing, skiing

**What is your hidden talent?**

I have learned through helping my 2 daughters that I can hold my own with pony tails, curling irons and hair straighteners.

**What is the best advice you have received and that you have used?**

Lead by example. Be the kind of leader that you would want to follow.

**What would be your advice for a new security professional?**

Learn from those around you that have been in the field and have experience. Continually learn and stay abreast of current trends and threats.

# Events

---

## 2016 Save the Dates

- Monthly Gartner Webinar: September (more details and the invitation will be sent out through the Security and Security-Officer mailing list)
- Secure World Dallas: September 27 – 28, Dallas, TX
- DIR Technology Forum: Tuesday, October 11, Austin, TX
- October 12 (afternoon): Threat Report Briefing by NTT Data, Austin, TX
- October 19 (9:30 – 10:30): Social Engineering presentation by Denim Group in the Capitol building, Austin, TX
- MS-ISAC Annual Meeting: October 30 – November 2, San Antonio, TX
- Innotech Austin: November 17, Austin, TX