

# THE DIR CYBERSECURITY INSIGHT

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

## Happy Holidays

### While You Are Away the Hackers Will Play...

The holiday season for state agencies and universities often means time away from the office and logged off the network. While time away from the desktop is much needed and well deserved, hackers who are aware of this absence will take advantage. Protect your agency and prepare a strong incident response plan before jetting away for the holiday.

Begin a discussion with the team to identify critical elements that will likely come into play in the event of an incident. What data do we have and what is at risk? Who will work the incident? Who needs to be notified? Answering these questions will become an essential part of the final incident response plan.

Here are a few steps to take when developing your incident response plan:

- Identify your data, its location and risk factors (consider who has access, what are the procedures around this and where might it be vulnerable)
- Develop a well-rounded plan including but not limited to:
  - Identify team members and their roles
  - Develop protocol for deferent types of attacks
  - Plan for an escalation process in the event of breadth or severity changes to the incident
  - Identify what parties need to be notified and the level of detail they are to receive
  - Develop protocol for collecting evidence
  - Set a time table for getting systems back online and returning business to normal
  - Document this plan and have it accessible in the case of system breach
- Exercise the plan
- Make changes based on discussions from the exercise
- Exercise the plan again
- Practice it one more time...

Now you are ready for a mostly relaxed holiday season. Rest (mostly) easy security friends. You are prepared.

### CONTENTS

#### Monthly Article

While You Are Away the Hackers Will Play **P.1**

#### Program Updates

InfoSec Academy **P.2**  
 Gartner Webinar **P.2**  
 NSOC Update **P.3**

#### Spotlight

Dr. David A. Abarca **P.3-4**

### EVENTS

#### Save the Date

- **TASSCC State of the State:**  
December 16, 2016, Austin, TX

- **Information Security Forum:** April 11-12, 2017, Palmer Events Center, Austin, TX

# InfoSec Academy Update

---

The next (and most likely last) opportunity to take the Texas Security Policy & Assurance course in a classroom setting is on Jan. 20, 2017. You must complete this course prior to starting any of the certification prep courses offered through the academy (Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), CompTIA Security+ and Certified Ethical Hacker (CEH). [Click here to enroll in the instructor led Texas Security Policy & Assurance class.](#) To learn about the Texas InfoSec Academy and course offerings, visit the [Texas InfoSec Academy](#).

## Gartner Webinars

---

In order to provide you with the ability to select a topic of the greatest interest and value to you, this month Gartner is providing a list of relevant on-demand security webinars from which to choose. To watch the webinar, please click on the underlined session title below, and you will be taken directly to it. You will also be able to download the presentation from the main landing page, as well. If you have any difficulties accessing the webinars, please send an email to Joe Martin ([joe.martin@gartner.com](mailto:joe.martin@gartner.com)). If you are interested in speaking with a Gartner analyst to interactively discuss the material presented in the on-demand webinar, please contact Steve Reda ([steve.reda@gartner.com](mailto:steve.reda@gartner.com)) to coordinate.

### Design a Modern Security Operation Center

Security operations are a critical component of an effective cybersecurity organization. Organizations pursuing a more mature security practice may decide to centralize all or part of those activities into a security operations center (SOC). This webinar details a structured approach to plan, establish and efficiently operate a modern SOC.

*Hosted by: Anton Chuvakin*

### Move Beyond 'Awareness' to Security Culture Management

On its own, security awareness can be ineffective in helping organizations instill the desired/needed values and behaviors. Employees need to be more than just 'aware' they need them to possess certain value frameworks, critical thinking skills and behaviors that are in-line with the organizations security policies. In this webinar, we outline the idea of proactive "security Culture management" an approach that contains aspects of security awareness, behavioral training/conditioning, marketing/messaging, systems of reinforcement, technology based guardrails, and more.

*Hosted by: Perry Carpenter*

### How to Build Your Next-Generation Mobile Security Strategy

Mobile attacks are becoming more advanced. Is it time to add more defense to your mobile infrastructure or just wall it off? BYOD versus COPE strategies are still highly debated.

*Hosted by: Patrick Hevesi*

## NSOC Update

---

The NSOC is dishing out security monitoring gifts this monitoring and security services!

season, providing its customers with additional

Ready and equipped to assist, the NSOC can implement additional monitoring and protection if a customer receives a threat targeting specific assets and at a specific time.

Below are examples of resources the NSOC can bring to bear on your behalf:

- Website monitoring
- Notification to our ISP's for additional DDOS mitigation
- Network Forensics Tool (NFT) preloaded with specific queries to alert on your assets
- An open source IDS sensor watching specifically your traffic
- NSOC Security analysts monitoring your specific assets

Additional countermeasures may be brought into action depending on the threat and the information provided. If you have a concern about a high-level event or received some information that you may be targeted for an attack, please contact the NSOC security team at [security-alerts@dir.texas.gov](mailto:security-alerts@dir.texas.gov) or 888-839-6762, and select option two. As with any event, the earlier we're made aware, the higher chance we'll have to assess the situation and determine what steps we can take before it kicks off. Thanks again and stay safe out there!

## Information Security Officer Spotlight

---



**Dr. David A. Abarca, CISSP**

**Assistant Professor and Information Security Program Director**

**Del Mar College**

### **Tell us about you.**

I have an AA in Liberal Arts from Del Mar College, a BS in Business Administration, a MS in Computer Information Systems, and an EdD in Educational Leadership.

I am an Associate Professor, and the Network Administration and Information Security Program Director for the Computer Science, Engineering, and Advanced Technology department at Del Mar College, a Hispanic Serving Institution, located in Corpus Christi, Texas.

### **What is your professional history?**

In 1977, I assisted a friend build an IMSAI 8080 from a kit he purchased and I was hooked on computing. Over the years, I built computers and learned to develop databases. I eventually went to work for IBM where I received a million dollar education for which I am eternally grateful. After leaving IBM, I started working for a technology service provider, and eventually, became a partner in the company. I started my own technology service consulting company and purchased a software company that developed IRS 1098/1099 reports and statements. I sold the

company and began a new career as an adjunct instructor at Del Mar College. I was later hired into a full time, tenure-track position teaching in the Computer Information Science Department, where I continue to teach today.

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

In the early days, Information Security was primarily locking the door! The massive mainframe computers required several people to connect, install, configure and maintain. ALL the data was produced by loading a stack of cards into the IBM 029 and punching holes in them!

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

My "customers" are students interested in preparing to enter the cyber workforce and the greatest challenge is helping them develop a broad conceptual understanding of security fundamentals so they will be prepared to interact with an everchanging series of platforms. While the syntax and composition of practical application will vary and

continue to evolve, the conceptual outcomes are similar.

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

Sharing my knowledge and experiences, and leading students through the development of critical thinking and research skills that will result in changing the economic trajectory of my students and their families.

**What would people never guess you do in your role?**

Helping veterans through their transition into the classroom.

**What other career would you have liked to pursue?**

Becoming a Rock Icon sounds like a challenging career, with lots of travel!

**What has been the greatest challenge that you have faced, and how did you resolved it?**

The biggest challenge is staying relevant to the technology with which you are interacting and supporting

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

I am proud of each of my students whom have found success in their career choice. Watching their experiences, here at Del Mar College, transform the economic future for themselves and their families.

**Top 3 life highlights.**

Falling in love and marrying my wife, sharing in the lives of our two children, and earning a doctoral degree.

**What are your hobbies?**

I read, fish, hunt, and play my piano and guitars in my spare time, and when I travel, my main hobby is landscape and wildlife photography. You may view many of photos at my website: [www.lensoftexas.com](http://www.lensoftexas.com).

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

I studied classical piano from the age of four through my first year in college.

**Any favorite line from a movie?**

"Are you going to pull those pistols, or whistle Dixie?" – from The Outlaw Josey Wales

**Favorite travel spot?**

I love traveling and photographing Shiprock, N.M., the Big Bend, Arches, Canyonlands, Rocky Mountain and other national parks in the southwest.

**Which CD do you have in your car? Or what radio station do you listen to?**

I usually listen to old 60's and 70's rock, classic C&W, 50's doo wop, and a little Big Band music.

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

My father lived an incredible life including his military service as Fire Chief for General Patton's 3rd Army Headquarters in Europe. He loved history and I would like to have learned more about his time in the service and as an Interpreter for numerous courts in South Texas.

**If you had to eat one meal, every day for the rest of your life, what would it be?**

Smoked/BBQ Chicken, Brisket, Turkey, Ham, Ribs, almost anything on a grill or in a smoker.

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

Start every interaction with, "How may I serve you today?" Many times people need more than "help" they need someone to be vested in their situation and the best way to do that is to enter into a situation with an attitude of "service to others". Service reaches further into developing and delivering just a solution. Oftentimes, "help" resolves only the immediate need rather than providing a deeper longterm solution that will resolve the cause of the situation.

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

Read, read, read, EVERYDAY! Read two articles everyday! One in your professional field and one to enrich your personal life! Each day that you fail to do this, is a wasted day that you will never get back. Even if you double your efforts tomorrow, you still did nothing to improve yourself TODAY, and you will never have THIS DAY again!

