



# DIR Cybersecurity Insight Newsletter

NOVEMBER FY2015 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

## Contents

---

### Monthly Article

Who handles your data?	2
Digital Era	3

### Texas Information Security Program Updates

InfoSec Academy	4
Incident Response	5

### Our State ISO Spotlight

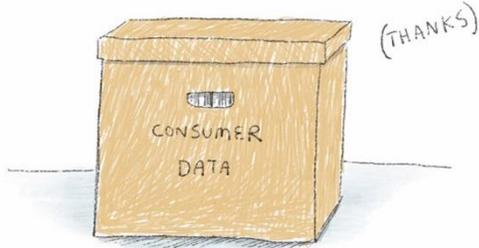
Marilyn Meador	6, 7
----------------	------

### From our State CISO

Incident Response	8
-------------------	---

Events	9
--------	---

PLEASE DON'T  
STEAL THIS.



Be Prepared, Be Ready.

# Who handles the life of your data?



Who is in charge of the process in your organization?

What is the role of Information Security in this process?

Usually the data lifecycle includes six phases from creation to destruction.

**Create:** This is probably better named Create/Update because it applies to creating or changing a data/content element, not just a document or database. Creation is the generation of new digital content or the alteration/updating of existing content. There are key considerations for the security program during data creation, such as identifying and classifying the data so that appropriate protections can be established from the onset.

**Store:** Storing is the act committing the digital data to some sort of storage repository and typically occurs nearly simultaneously with creation. The security program now needs to consider the data at rest and how it will be protected, monitored, and how access restrictions will be implemented. Other security program considerations are the backup and recovery processes to ensure that data availability is ensured.

**Use:** Data is viewed, processed, or otherwise used in some sort of activity. Use should be limited to only that which is approved and authorized, so identity and access management become an integral component of data use. Additionally, the architecture of the system that provides access must be considered to ensure that internal and external access requirements can be met. Additionally, the ability to detect misuse becomes pivotal.

**Share:** Data is exchanged between users, customers, and partners. Once again, the appropriate and authorized access should be considered, but now the complexity of where the data will now reside as it may be copied, replicated, modified, and used for additional purposes should also be considered. Extending requirements of protection to third parties introduces expanded elements to the security program.

**Archive:** Data leaves active use and enters long-term storage. The design of the original system hopefully include all of the required protections, monitoring, and detection, as well as response and recovery needs. However, archiving now introduces alternative media types and potentially offsite facilities. The security program must consider data in the archival stage.

**Destroy:** Data is permanently destroyed using physical or digital means (e.g., cryptoshredding). When the time comes to remove the data from the environment at the end of the lifecycle, it is critical to consider all of the copies and replicas, alternative media types, and partners that may now also have the data. Identification at the beginning of the lifecycle is extremely important to completely accomplish secure destruction, and the manner in which destruction occurs must be capable of truly ending the data lifecycle.

# Security 101 – Digital Era

## What happens to your data when you leave?

Studies show that in 2010, data stored worldwide accounted for 1.2 ZB. By 2015, the estimated size is will be 7.9 ZB and 40 ZB in 2020. How can we protect it all?

*Source: IDC, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East (Dec. 2012)*

Times have changed, and when we used to worry about important documents such as wills or income tax reports, we stressed the use of safe boxes. Today, everything is on the Internet, in the cloud, in our hard drives, on USB drives, and so on. How many of us don't carry a piece of paper for our auto insurance anymore? How many of us pay for our morning Starbucks using a mobile app that recharges automatically since our credit card information is saved? And how many of us use a password keeper app that requires a master password?

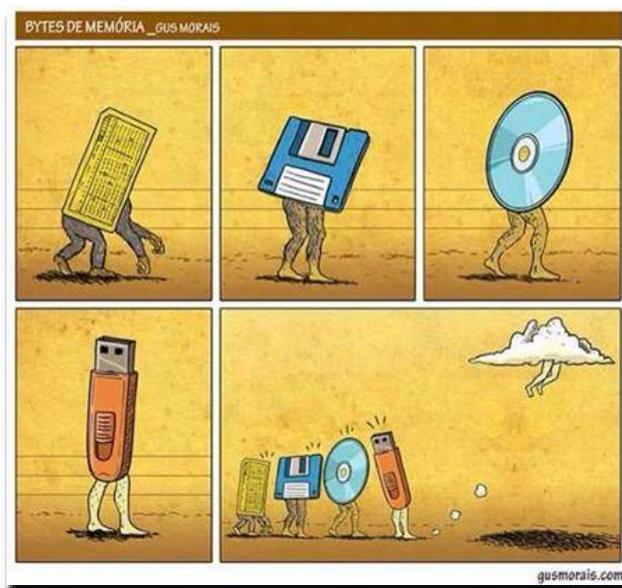
One part of the CIA triad is Availability – availability of the systems and security. But what about us? What about ourselves? What if something happens to us and nobody else knows how many accounts we are leaving behind? Where is our story? Will it die with us?

Last month I started compiling a list of all my email accounts, and I think that I came up with 10 (very reasonable, isn't it?). One related to my kids, one for professional stuff, one for friends, one for snooping about, and others if I keep going.

I read an article that has been on my mind for several months now, since I saw a former classmate in my Facebook account listed in the *people that you might know* section. This person passed away a couple of years ago. The article, [What Happens to Your Data After You Die](#), offers three very useful tips:

1. **Make an inventory of all your digital assets.** That includes the documents on your computer, the photos on your phone, all data stored on thumb drives or backup disks, and every online account, including the ones you no longer use. It's a big job, but you don't have to do it all at once. Start with the most important things and work your way down the list. Odds are your primary email account will be number one, since that's typically where online accounts send password resets. Keep reading for advice on where to store this data.
2. **Figure out what you want to happen to all of this stuff after you're gone.** Do you want your family to have access to all your emails? How about photos? Videos and other material you've downloaded? There may be some things you don't want your loved ones to see. Decide now, and make your wishes known to those you care about.
3. **Assign someone to be your digital executor.** Be explicit in your will about what you want to happen to your assets. Don't assume your survivors automatically have a right to it all, because the law varies greatly from state to state. The blog The Digital Beyond offers some [sample power-of-attorney language](#) to include in your will.

It is good security practice to use different accounts for different functions, but more importantly it is good to have control over those accounts.



# Security Program Updates

## Texas InfoSec Academy

### *Texas InfoSec Academy Launches*

The Office of the Chief Information Security Officer is excited to announce the launch of the Texas InfoSec Academy on November 3, 2014.

The InfoSec Academy includes an LMS that hosts all of the available courses. Currently over 250 soft skills courses are available. Over the next few months, additional courses will be added to ultimately include six different security course tracks, the Texas Security Policy & Assurance course, and security certification preparation courses. On Friday October 31, eligible participants were emailed a link to the learning management system (LMS) along with their username and a temporary password.



### *Soft Skills Courses*

A variety of soft skills courses are available covering a wide range of topics. Examples of available course titles are Team Building Without Time Wasting, Helping Employees Use Their Time Wisely, and Everybody Wins: How to Turn Conflict into Collaboration.

### *Security Courses*

Six different tracks of security courses will be offered, giving the learner the opportunity to choose a track based on their area of interest. The tracks available are IS Management Leadership, Incident Handling, Forensics, Disaster Recovery, Application & Secure Code, and Penetration Testing & Hacking. Once a learner finishes a track, they may take courses on a different track. These courses will be phased into the LMS beginning in mid-November 2014.

### *Texas Security Policy & Assurance*

The Texas Security Policy & Assurance course is designed to prepare security professionals to apply the state rules regarding information security within their agency and to enable them to better serve their agencies and the citizens of Texas. The course curriculum includes modules on Texas rules and legislation, data classification, security framework, agency security plans, and reports. The CISO/ISO of each agency or institution of higher education is required to take this course. This course will be offered via instructor led training and will also be offered online.

### *Certification Preparation Courses*

Once the learner has taken the Texas Security Policy & Assurance course, the first two courses on the security course track that they have selected, and one soft skills class, they will be eligible to take certification preparation courses. Prep courses will be offered for the following certifications: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), and Certified Ethical Hacker (CEH).

If you have any questions about the Texas InfoSec Academy, please email: [dirsecurity@dir.texas.gov](mailto:dirsecurity@dir.texas.gov)

[Texas InfoSec Academy Website login](#)

## Incident Response Exercises

The Department of Information Resources Office of the Chief Information Security Officer is pleased to offer monthly tabletop security exercises in partnership with the University of Texas at San Antonio's Center for Infrastructure Assurance and Security (CIAS). There are several items you need to participate in these exercises.

You will need a login ID to the CIAS Learning Management System (LMS), which hosts the instructional classes on how to participate and the exercises themselves. The link to the LMS is [https://txdir.learnupon.com/users/sign\\_up](https://txdir.learnupon.com/users/sign_up)

Each agency or institution of higher education should designate an exercise planner. Exercise planners should take the classes on the LMS, coordinate your organization's exercise, gather information for the after action report, and send a summary of the results to DIR so we can incorporate your lessons learned into our statewide security offerings. The classes are:

- Introduction to Exercise Planning – 30 minutes
- Exercise design and evaluation – 1 hour
- Exercise Logistics – 15-20 minutes
- Exercise Material Review - 5-10 minutes

The monthly exercises will be on the LMS. We will send an announcement when the exercises are available.

To keep things relatively simple for participants, CIAS created a "course" on the LMS that contains all supplemental documents for the initial exercise. Once the participant registers for the LMS, he/she will see the exercise listed as an available course. The following materials are located in that course:

1. Exercise introductory PowerPoint slide deck
2. Links to the exercise online videos. These are hosted on a private YouTube channel. Click on *Course Description* to see these links.
3. After Action Report / Improvement Plan template
4. Online Exercise After Action Report / Improvement Plan Debrief to be sent to DIR
5. Exercise Participant Message Worksheet
6. Exercise Development Guide (completed for this exercise)

It is very important that you send the completed debrief template to DIR on a monthly basis so we can see who is using these exercises and what impact it is having on the overall state security program. Please send this to [DIRSecurity@dir.texas.gov](mailto:DIRSecurity@dir.texas.gov)

If you have any questions or concerns, please contact us at [DIRSecurity@dir.texas.gov](mailto:DIRSecurity@dir.texas.gov)

# Information Security Officer Spotlight

## Marilyn Meador Information Security Officer Tarleton University

Marilyn graduated from Texas Woman's University with a Bachelor of Science in Government/Legal Studies.

### What is your professional history?

Retired from Frito-Lay/Pepsico after 30 years. I started out in the Accounting Department at Frito-Lay. The last few years I was a Project Manager for IT technical projects. Then my husband and I moved to Stephenville, and I was hired as the Information Security Officer at Tarleton State University as a result of my technology and project management/compliance experience.



### How did you come to the security field?

Tarleton needed an IT Security Compliance Officer, and my background in the overall understanding of IT operations and infrastructure served me well. I had also served on the Sarbanes-Oxley IT Audit Team for PepsiCo.

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

Information security has changed from just protecting a piece of technology to tracking data to protecting it regardless of the technology.

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

Everyone that uses technology on campus is my customer. The most challenging area for me is trying to keep people updated and aware of security and privacy and how their actions play a big role in it. It is a moving target most days.

### How did you first learn about Tarleton University?

I knew about Tarleton from when I was in college out in Alpine, Texas, at Sul Ross. TRLSU's rodeo team always beat ours.

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

The people

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

Had the timing been different, I would like to have gone on to law school as planned. I always wanted to be a prosecuting attorney.

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

Running an international technology project for PepsiCo that had over 100 FTEs in two countries and spanned one year.

### Tell us about your most proud accomplishment.

I got an award and a bonus at PepsiCo for bringing the above project in on time and on budget.

### Top 3 life highlights.

When my two kids were born and the 20 years I had married to the love of my life before he passed away last year.

### And where did you grow up?

Born in Pecos, Texas, and attended high school in San Angelo, Texas.

Do you have family in Austin?

Yes, my daughter Kasi, her husband, and my grandson live in Austin.

What are your hobbies?

I enjoy going to the movies and reading.

People would be surprised to know that you...

I taught karate/self-defense when I was younger. My family still owns the ranch out in west Texas that Poncho Villa used to ride across when the law was chasing him. And as scary as it may be to some people, I have a twin sister.

Any favorite line from a movie?

"I'll be your Huckleberry" from the movie *Tombstone*.

Are you messy or organized?

Organized.

Favorite travel spot?

Not sure I have a favorite; I just like seeing America.

What books are at your bedside? Or which one was the last one you read?

The Bible.

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

Dwight Yoakum. I like good old-style country music.

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

John Wayne.

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

Mexican food.

Least favorite food?

Greek.

If you were to write a book about yourself, what would you name it?

Been There, Done That. I have had an amazingly full and wonderful life.

Describe what you were like at age 10.

Very shy and afraid of people.

What is one thing you couldn't live without?

Freedom.

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

Children learn what they live.

What would be your advice for a new security professional?

Try not to get overwhelmed with all the information and know when to tell people, "It isn't a security thing." Not everything is.

<b>Tarleton's General Information</b>
<b>Established</b> September 4, 1899
<b>Joined A&amp;M System</b> 1917
<b>Colors</b> Purple and White
<b>Mascot</b> Texan Rider
<b>Nickname</b> Texans
<b>Athletic Affiliation</b> Lone Star Conference
<b>Fall 2014 enrollment</b> 11,700+
<b>Number of faculty</b> 578
<b>Number of staff</b> 506

## Tarleton University

With its main campus in Stephenville, an hour southwest of Fort Worth, Tarleton State University offers the value of a Texas A&M University System degree with its own brand of personal attention, individual opportunities, history, tradition and community.

# Insight from our Texas CISO

I continue to hear the phrase “it’s not a matter of if, but when” in the context of cybersecurity incidents and data breaches. Interestingly enough, I hear this in conversations occurring at executive leadership levels, which is a positive indication that those outside of the security profession are starting to realize the complexity of the objectives of information security. But I would like to provide a word of caution as this phrase becomes a mantra: if it is a matter of when, when it happens, you must be prepared to respond.

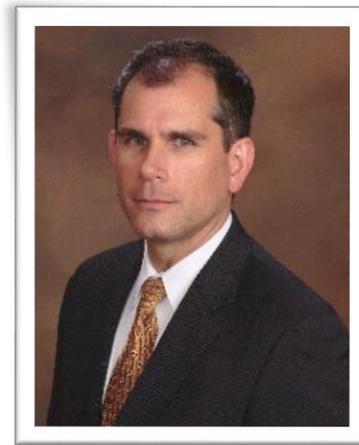
In several of the articles I have written for our Insights Newsletter, I have reinforced the five functional areas of the Texas Cybersecurity Framework: identify, protect, detect, respond, and recover. This month I want to focus on response, because a capable and coordinated response will be critical if you are to survive the “not if but when” occurrence of a significant cybersecurity event.

Now that our leadership understands that these events will happen, they trust us as the experts to lead them during the incident and provide them with necessary information to make critical business decisions. If trust is to be maintained during and following a cybersecurity incident or significant data breach, competence must be conveyed throughout. In order to have a competent response, preparation is the key, or perhaps through constant trial by fire and continual improvement processes. Fortune favors the prepared mind, while live fire continual response may only produce a weary mind.

I had the opportunity during October to participate in a Global CISO Summit and host a roundtable discussion on rebuilding trust after a cybersecurity incident. The room was filled with many highly effective and seasoned CISOs, and, as strategic thinkers are apt to do, the conversation went to preparation rather than execution. In other words, preparation and incident response exercises were consistently referred to as the best form of ensuring competency, and competency leads to trust. I heard numerous examples of lessons learned from the exercises that nearly all of these participants conduct on a monthly basis. And their exercises continue to produce learning moments.

There are a variety of ways to conduct incident response exercises, and, like any competitive sport, practice is very important if you are going to succeed. I hope that you are able to utilize the scenario packages we have begun to provide this month, and I look forward to hearing your stories and any feedback that you provide. The format is meant to be flexible, and the feedback forms are there to share the things you learn with others.

I also prepared a session that was part of the Texas CIO Academy here in Austin on November 6 that helped us advertise this new offering. Please help us spread the word. The OCISO is hopeful that we can use this offering to help you improve your incident response, because fortune favors the prepared!



*Brian Engle  
CISO, State of Texas*

Brian Engle

# Events

## DIR participation in Cybersecurity Events

- Brian Engle, State Chief Information Safety Officer (CISO), participated at Texas Public CIO Academy  
**Date:** Thursday, November 6, 2014  
**Location:** Hilton Austin  
[www.govtech.com/events/Texas-Public-Sector-CIO-Academy.html?page=agenda](http://www.govtech.com/events/Texas-Public-Sector-CIO-Academy.html?page=agenda)
- Brian Engle, State CISO will be providing remarks and participating in the in a DHS CSF event in Houston.  
**Date:** Monday, November 10, 2014  
**Location:** Houston, Texas  
[www.dhs.gov/ccubedvp](http://www.dhs.gov/ccubedvp)

## Training and Conferences Around the State

### *Monthly Security Program Webinar*

Network Security for Private and Hybrid Clouds

**Date:** Thursday, November 13, 2014

**Time:** 10:00 am CDT

[www1.gotomeeting.com/register/978692256](http://www1.gotomeeting.com/register/978692256)

### *BSidesDFW*

**University of Texas at Dallas**

**Date:** Saturday, November 8, 2014

**Location:** University of Texas at Dallas (UTD)

[www.securitybsides.com/w/page/79986053/BSidesDFW](http://www.securitybsides.com/w/page/79986053/BSidesDFW)

### *Security Today Conference and Expo*

**Date:** November 17-19, 2014

**Location:** Gaylord Texan Resort, Dallas

[security-today.com/events/st-2014/home.aspx](http://security-today.com/events/st-2014/home.aspx)



Feedback, comments, stories, etc.

[DIRSecurity@dir.texas.gov](mailto:DIRSecurity@dir.texas.gov)



Office of the  
CHIEF INFORMATION  
SECURITY OFFICER  
State of Texas