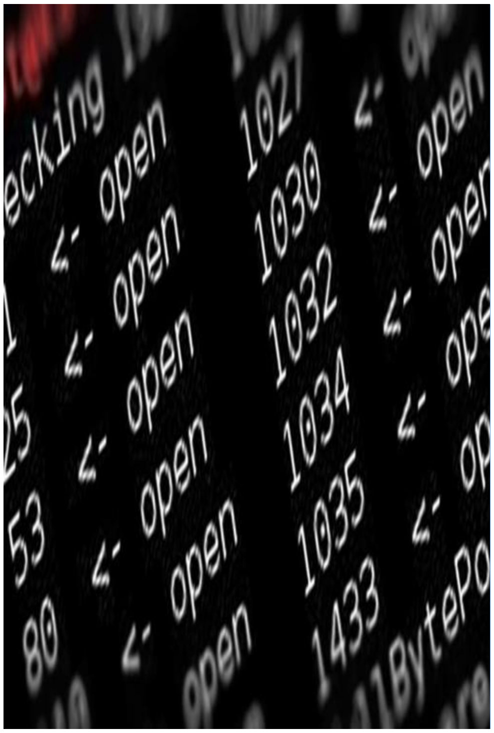
# DIR Cybersecurity Insight

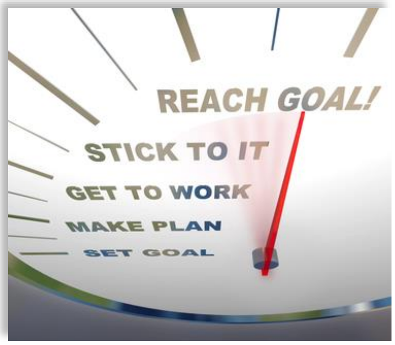
## Newsletter



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

## New Fiscal Year

The OCISO has goals for several initiatives in the new Fiscal Year.



- OCISO launched this newsletter in 2014, and we will continue to expand and improve the articles through FY 2015. We will also start distributing the newsletter to a broader, non-security audience.
- The SANS Securing the Human End User training that OCISO piloted during FY 2014 has been expanded from 30,000 seats to 90,000 seats, letting agencies cover more of their employees.
- The Governance, Risk, and Compliance platform will be launched in FY 2015.
- The InfoSec Academy is launching in October 2014.
- The revised TAC 202 should be approved and in effect in February 2015.

We've laid out our goals. Are you ready with yours?

### Contents

Security 101

Texas Information Security Program Updates

Our State ISO Spotlight

Collaboration Opportunities

From our State CISO

# Security 101 – Incident Response Plan

## What's in Your Plan?

Have you started one? If so, what is the status? Who is in your plan? Have you tested it?

*When an incident occurs, many incident response plans fail because most generally focus on how to avoid an incident, and we fail in the response planning phases.* ***How do you recover? How do you contain? What is the impact?***

## Definition of Incident Response

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to manage the situation in a way that limits damage and impacts and reduces recovery time and costs.

## Common Steps in an Incident Response Plan

1. Preparation: The organization educates users and IT staff of the importance of updated security measures and trains them to respond to computer and network security incidents quickly and correctly.

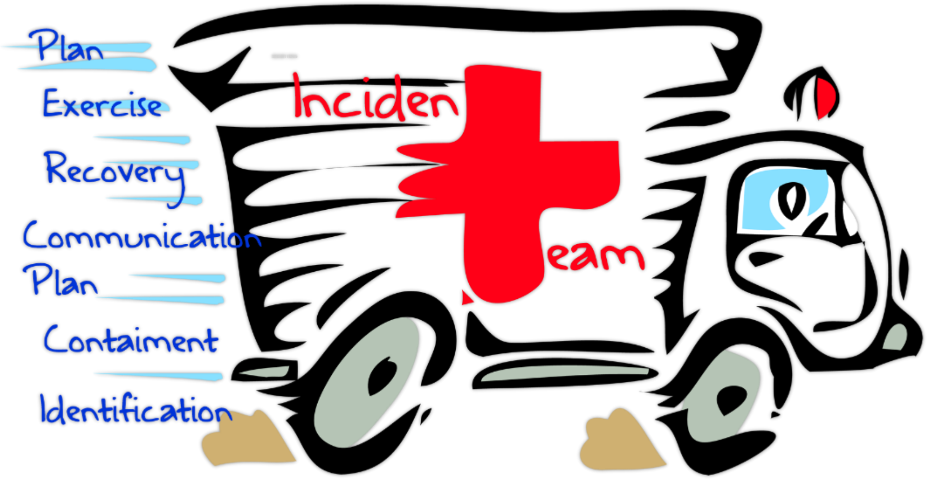
2. Identification: The response team is activated to decide whether a particular event is, in fact, a security incident. The team may contact the CERT Coordination Center, which tracks Internet security activity and has the most current information on viruses and worms.

3. Containment: The team determines how far the problem has spread and contains the problem by disconnecting all affected systems and devices to prevent further damage.

4. Eradication: The team investigates to discover the origin of the incident. The root cause of the problem and all traces of malicious code are removed.

5. Recovery: Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for any sign of weakness or recurrence.

6. Lessons learned: The team analyzes the incident and how it was managed, making recommendations for better future response and for preventing a recurrence.



### Steps for an Incident Response Plan.

According to NIST Guidelines

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post Incident Activity

# Security Awareness and Education

## Response Back to the Incident!

The SANS Institute recently published survey results titled "Incident Response: How to Fight Back."

The study found that only nine percent of organizations believe that their response to security incidents is "highly effective." More than a quarter of those responding said they were dissatisfied with their incident response (IR) capabilities, calling them ineffective.

The most cited obstacle to effective IR processes was lack of time to practice response procedures (62%), speaking to the need for both hands-on walk-throughs and mock exercises that test written policies and aid in standardizing triage and response in enterprise incidents.

This study underscores the need for security practitioners to test their incident response capabilities and perform follow up analysis. DIR, in partnership with the University of Texas at San Antonio Center for Infrastructure Assurance and Security (CIAS), will be offering monthly cyber security exercise scenarios ("Exercises"), associated questions/surveys and basic instructions. DIR will also provide template after action reports for each scenario. Each state agency/university can use this Exercise Kit to conduct an exercise over the course of two days each month and send a completed debrief template to DIR, so that we can compile and share results and lessons learned from each exercise.

To ensure the highest level of quality and maintain consistent and productive exercises, DIR will provide a course for exercise planners. This class will familiarize planners with the exercise kit and other tools needed to conduct these exercises. This will be an online course that can be taken according to the agency's timetable.

## SANS Securing the Human Training Program Updates

The *SANS Securing the Human End User* training program has been extended through October 31, 2015. If your agency is not already taking part in this program, please contact DIRsecurity@dir.texas.gov for more information.

SANS offers several free resources to help create and enhance your security awareness program. Visit www.securingthehuman.org and click on the *Resources* link.

Among the free resources is the *Measuring Human Risk Survey* at www.securingthehuman.org/resources/metrics. It's a free 30-question survey that you can use to measure your organization's security awareness posture. Before launching your *Securing the Human End User* training program, submit this survey to your staff, and then use the answers to create a baseline. When training is complete, submit the survey again to gain an idea of just how much your staff has learned.

## Texas InfoSec Academy for Information Security Officers

After months of planning and developing this academy, it is almost ready to be launched.

In October 2014, in alignment with the National and State Security Awareness month, OCISO will be launching the infosecacademy.texas.gov learning management system. ISOs from state agencies and higher education institutions will be able to complete four different pillars comprising the entire academy: InfoSec Core, Software Skills, Policy and Assurance for Texas, and Security Certification camps.

# Information Security Officer Spotlight

## RICHARD MARTIN, CISSP, CHFI, CISA, CIA

### DIRECTOR OF INFORMATION SECURITY AND COMPLIANCE

### TEXAS STATE TECHNICAL COLLEGE

*I'm a very proud graduate of Baylor University, class of 1995 (Sic'Em!). After bouncing around in the logistics industry for a time finally found a home as an internal auditor for a publically traded company based in Austin. I hold designations of CISSP, CHFI, CISA, and CIA.*

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

My path to information security has been the non-traditional route for sure. As an auditor, I would review various types of IT controls (general and application, depending on scope), and my curiosity kept leading down the path of trying to understand more and more of what was really happening. After arriving at TSTC, I began auditing IT and then moved to Enterprise Risk Management where I worked directly with IT on risk and controls.

That eventually led to my current position as ISO two years ago. My CTO (Rick Herrera) jokingly tells management that he brought me in to fix all the things I pointed out in my audits. He and management took a bold gamble, and for that, I am very appreciative.

### How did you first learn about TSTC?

I grew up in Waco, so TSTC was well known to me. It wasn't until I started working there that I grasped the immense importance of TSTC's mission. We have the motto "We Change Lives," and I truly believe that and have seen it, first hand.

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

For me it has been a shift in the deployment of resources. Like many others, I tended to focus heavily on proactive/preventative measures along the perimeter. In the past six months, I have worked closely with our Director of Infrastructure (Rick Collatos) and the Director of Support Ops (Shelli Scherwitz) to shift some resources to reactive/detective controls.

That shift is based on an adaptive security model, but more importantly it comes from a philosophy that all devices are vulnerable, whether we know it or not. That belief brings all devices within scope, not just the ones that are listed as vulnerable by scanning tools. That philosophy completely changed our risk assessment methodology.

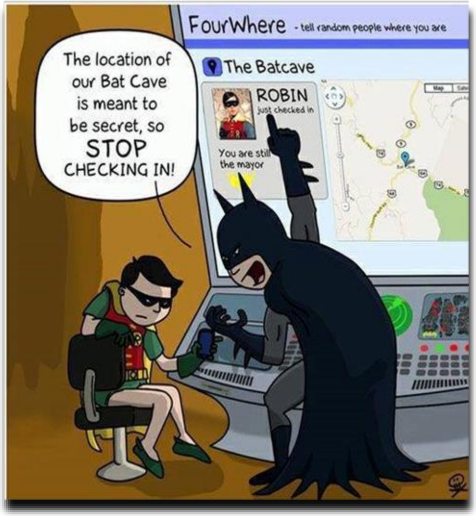
### What do you like best about your job?

Because TSTC offers degrees in Digital Forensics and Network Security, it is tremendously rewarding to interact with the students who are studying in those fields. It's a truly unique experience where the students have an opportunity to learn the latest tools and techniques in the classroom and occasionally get to compare that to a real-world security shop. This semester we hope to start a Forensics and Security club for the students where we can merge and share even more knowledge.

Equally rewording is the opportunity to work with the IT technicians. I am truly fortunate to be associated with some extremely gifted and brilliant individuals.

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

Batman!!


FourWhere - tell random people where you are
The Batcave
ROBIN just checked in
You are still the mayor
The location of our Bat Cave is meant to be secret, so STOP CHECKING IN!

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

My primary customers are anyone associated with TSTC, be it our students, faculty, staff, Board, or alumni. The biggest challenge I face day-to-day is communication. I rely on our users to help me defend our resources. But as with many ISOs, I run the risk of either over or under communicating, depending on the threat. It's a delicate balance and quite often hard to judge.

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

When I came into position, IT had just begun to consolidate from four independent shops (one at each main location) to one statewide fully integrated function. The policies and procedures were ancient to say the very least, and some had not been reviewed in 20 years. There were polices that conflicted with regulation, procedures that conflicted with policy…it was a mess. On top of that, the leadership at each one of the four main locations had differing priorities and objectives with regard to IT.

Working with our Solutions Director (Dennis Burrer), we were able to start hammering out a governance model of system and data owners and policy to reinforce a governance model that management could accept. We have designed that to be as nimble as possible.

Even with all of the challenges, mistakes, reworks, and disasters, we continue to have very clear and concise "tone-at-the-top." Without that, all of our efforts would be lost.

### Tell us about your most proud accomplishment?

When the fertilizer plant exploded in West and devastated that community, the entire TSTC family pulled together in a concerted effort to ease the suffering of those residents. Being a small part of that was extremely rewarding and very humbling. Chancellor Reeser, President Stuckly, and our Board of Regents took decisive action and opened up our housing to residents that were displaced. When I think about the first three days of that event, I am still amazed at how quickly the TSTC Waco location mobilized in support.

### Top 3 life highlights

1. Graduation from Baylor University
2. Living through my 20s and 30s
3. Being ISO

### And where did you grow up?

I grew up and have spent most of my life in Waco with brief stints in Colorado Springs, Tulsa, and Indianapolis.

### Do you have family in Austin?

I have a lot of friends in Austin who I consider family. Especially TSTC's Application Development Director, Jack Simonton (love ya, buddy).

### What are your hobbies?

My hobby is really what I do for a living. Information security is just really interesting to me. I often joke that if my eyes are open, I'm scanning something.

### People would be surprised to know that you…

1. I have three Star Trek uniforms (That's right, three).
2. I buy, rent, and sell residential property.
3. I have a collection of name tags and badges from all of my travels.

### Any favorite line from a movie

"You, boy, are arrogant, hot tempered and entirely too bold. I like that. Reminds me of me." –Porthos, Three Musketeers.

### Are you messy or organized?

My office is a wreck. My truck is the same way.

### Favorite travel spot?

Without a doubt…VEGAS!

### What books are at your bedside?

I am currently reading the DC series "Damian: Son of Batman." I pretty much stopped reading books after Michael Crichton passed away.

### What is the CD that you have in your car?

Like most Texans, I have Robert Earl Keen queued up quite often. But I have been getting into this surf band out of Austin called the Nematoads. (The guitar player, Ted James, is amazing!)

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

Audie Murphy

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

Enchiladas!!

### Least favorite Food?

Those damn rice cake things.

### If given a chance, who would you like to be for a day?

Batman!

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

Entropy: My Life's Story

### Describe what you were like at age 10

Oooff…1983…those memories reached the end of their retention period several years ago.

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

Don't get caught up in what you can't control. Focus on what you can control and trust the universe will work out as it should.

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

1. Have thick skin and an open mind.
2. Don't take yourself too seriously.
3. Your opinion is just that.
4. Understand what risks are truly material to your organization.
5. Prepare for the worst. It will happen.
6. When in doubt, call Ted or Eddie.

# Collaboration Opportunities

**The Statewide Information Security Advisory Committee (SISAC)** provides guidance to the Texas Department of Information Resources (DIR) on the Statewide Information Security Program. The committee, chartered by DIR in 2011, is comprised of information security professionals from state and local government and representatives from private industry.

## What's up with the Privacy Subcommittee?

We are about to launch into our fourth year in September! It's hard to believe, but it seems like only yesterday that Karen Robinson (the CIO for Texas) and Angel Cruz (then CISO for Texas) embraced the idea of allowing state government privacy professionals to become actively involved in helping with the framework of the state's information protection strategy. Since that date, Brian Engle became the state's new CISO and has become a robust supporter of our initiatives!

Throughout our history, the subcommittee has met on a regular basis to discuss current events and trends that teach us how to collaborate with stakeholders and add value in our respective home agencies. Not only do we network and exchange lessons learned but we also help each other create work products that can be adapted for use by any agency. A few of our past accomplishments include:

1. A written Incident Response Plan, to which we affectionately refer as "the Red Book," which will be distributed and discussed at our September 2014 meeting.
2. A Data Classification Template that is currently available on DIR's website.
3. Proposed classification and job descriptions for three different levels of Privacy Analysts (B21, B23, and B25), currently pending review and approval by the State Auditor's Office for potential submission to the 84th Legislature.
4. And, pending for this coming year, we have enough volunteers for prepare a much needed template for uniform contract terms and conditions for privacy and security controls, including those for cloud computing.
5. I'd like to give special recognition to the Chairs of our former Task Forces**:** **Sheila Stine** (newly appointed Chief Privacy Officer for HHSC) and **Martin Zelinsky** (General Counsel for DIR), for the Red Book Task Force; **Lona Chastain** (Assistant General Counsel and Open Records Coordinator for the Texas Workforce Commission) for the Proposed Revisions to the Public Information Act for potential consideration by the 83rd Legislative Session; and **Nancy Pleasant** (Privacy Advisor for the CPA's Chief Privacy Office) who lead *two* task forces to a produce a relevant product: the Data Classification Template and the drafts of the three classifications and job descriptions for Privacy Analysts I-III.

In the coming year, we may also have capacity for another task force, depending on how popular the topic might be. So please feel free to contact me if you are interested in being a part of or even leading a group of professionals in a task force that could create an additional resource for state privacy professionals. Meanwhile, it's always exciting to anticipate the activities of our lawmakers during session but especially during an election year. We know that means that work gets busier for some of you, but we welcome you to any of our events that you're able to attend! Please remember to email me at Elizabeth.Rogers@cpa.state.tx.us for topic ideas that we can include on our agenda or for any leadership roles you'd like to have for task forces related to other topics. And, as always remember to *Keep it Private!*

*Elizabeth Rogers*
*Chair, Privacy Subcommittee of the DIR Statewide Information Security Advisory Committee*
*Chief Privacy Officer*
*Comptroller of Public Accounts.*

**Communications Subcommittee**
Frosty.Walker@tea.state.tx.us
ISO, Texas Education Agency

**Privacy Subcommittee**
Elizabeth.Rogers@cpa.state.tx.us
CPO, Texas Comptroller of Public Accounts

**Security Workforce Development**
Jesse.Rivera@cpa.state.tx.us
CISO, Texas Comptroller of Public Accounts

**Risk Assessment Subcommittee**
Shirley.Erp@hhsc.state.tx.us
CISO, Health and Human Services Commission

**Policy Subcommittee – (membership currently closed)**
Edward.Block@dir.texas.gov
Deputy CISO, Department o of Information Resources

**Solutions Subcommittee**
Claudia.Escobar@dir.texas.gov
Statewide Security Services Delivery Lead, Department of Information Resources

Join a Team

# Insight from our Texas CISO

*Brian Engle*
*CISO, State of Texas*

As we prepared this month's Insight newsletter, privacy was a hot topic in more ways than one. State agencies, higher education institutions, and local government organizations all interact with citizen information as an integral part of our missions. Security programs place a high degree of importance on confidentiality, and we absolutely include integrity and availability as equally important pillars. But what about privacy?

The convergence of security and privacy has brought many celebrities into a different limelight here in these last days of summer. An interesting mix of technical vulnerability, cloud technology, and of smartphone devices has placed information once thought private into a very public realm.

In another facet, findings from the Nationwide Cyber Security Review survey developed by the US Department of Homeland Security in cooperation with the Center for Internet Security, National Association of Counties and National Association of State Chief Information Officers found that privacy was the least mature area of all control areas for states, state agencies and local governments. Approximately 50% of the respondents to the survey indicated that controls related to privacy were performed at an ad hoc level, with some degree of processes and standards documented, but few were operating at a risk managed level.

Policies that provide guidance to ensure that only the necessary data is collected and used for the specific purposes for which it was collected is important, and likely beyond what a typical security policy defines. Additionally, and essential to establishing citizen trust is making these practices available to the public and demonstrating how the governance and monitoring of a privacy program occurs. Take a look around your organization and consider how privacy is accomplished.

It was great to get an update from Elizabeth Rogers on the Statewide Information Security Advisory Committee's Privacy Subcommittee. I look forward to working more with our state privacy experts, and hope you will help us to focus strategies around this very important area. Privacy has so many connections to information security, but the issues that we see in privacy risk really do require a distinct approach. Keep an eye out for this topic in upcoming months as we dig in deeper and see how we can raise the bar for Texas citizen privacy.

Brian Engle

# What's coming down the pike?

## Monthly Security Program Webinar

**What**: Keep Privacy in Mind When Developing Mobile Protection Programs
**Cost**: Free
**When**: September 23rd, 2014.
**Time**: 2:00 pm CDT
**Info**: www1.gotomeeting.com/register/940092568

## CISSP Training Class

**When:** October 2-24, 2014
**Location:** Stephen F. Austin Building, Austin
**Info:** Contact Brandon Roger (Brandon.Rogers@glo.texas.gov)

## InnoTech Austin

**When:** October 15, 2014
**Location:** Austin Convention Center
**Info:** www.innotechconferences.com/austin/

## Houston Security Conference (Hou.Sec.Con)

**When**: October 16
**Where**: Derek Hotel, Houston
**Info**: houstonseccon.com/v5/

## BSides Houston

**When**: October 18, 2014
**Where**: Site TBD, Houston
**Info**: www.securitybsides.com/w/page/81064187/BSidesHou
Full list of Texas BSides events at: bsidestexas.blogspot.com/

## We would like to hear from you.

Give us your feedback!

DIRSecurity@dir.texas.gov

Office of the CHIEF INFORMATION SECURITY OFFICER State of Texas