



DIR Cybersecurity Insight Newsletter

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

Do you have your Cybersecurity resolutions for 2015?

- ✓ **Identify**
- ✓ **Protect**
- ✓ **Detect**
- ✓ **Respond**
- ✓ **Recover**

Contents

Monthly Article

Protect yourself these Holidays 2

Texas Information Security Program Updates

Incident Response 3

InfoSec Academy 4

Network Security Operations Center Update

5

Our State ISO Spotlight

Sean Miller 6, 7

From our State CISO

Incident Response 8

Events 9

Protect yourself for the Holidays



Online shopping, online protection of your info. How?

- **Shop only on secure Internet connections:** Do not conduct any transaction that involves personal, financial or credit card information while using an open and unsecured Wi-Fi connection. Unsecured connections are common in public spaces such as transportation hubs, municipal hotspots, and in stores and coffee shops.
- **Only process payment on HTTPS web pages:** When entering payment information online you should verify that HTTPS (not the usual http) is in your website address bar to protect yourself from identity thieves and cyber criminals.
- **Do not be tricked by confusingly similar website and domain names:** Pay particular attention to your retailer's URL when shopping online. Scammers use variants of a known company's Internet address to try and lure users into visiting fake websites. Avoid clicking on links from email or social media sites.
- **Protect yourself by using credit cards:** With the advent of point-of-sale malware and rampant data breaches, identity thieves are now more sophisticated and dangerous than ever. If you are going to make purchases online, you can best protect yourself from the risks of identity theft and fraud by using credit cards.
- **Be wary of too-good-to-be-true contests and prize promotions:** Consumers should be suspicious of any email, messages, or posts on social networks promoting giveaways or contests that seem too good to be true, e.g., free high-value gift cards, tablets, and smartphones. These "contests" are often scams designed to bilk consumers out of money and/or to collect consumers' personal information for resale.
- **Read the fine print:** Broadly worded promotional offers and advertisements often mislead consumers into paying full price for items they believed were on sale.
- **Watch out for hidden shipping costs:** It is common practice for Internet retailers to advertise prices that do not factor in shipping and handling.

Program Updates

RSA Archer GRC Update

Security Incident Reporting

Security Incident Reporting is rolling out on January 2, 2015. Agencies and Higher Education Institutions will be able to record and track all of their incidents in RSA Archer. Urgent incidents should be submitted using the Archer system to ensure required escalation to DIR. Urgent Incidents are incidents where confidential data was compromised, incidents reported to law enforcement, or incidents that can propagate to other agencies. Agencies and Higher Education Institutions using Archer for all of their incident tracking will automatically have urgent incidents escalated to DIR. Both Security Incident and Monthly Reporting use Veris data elements for submission to the Verizon Data Breach Report.

Monthly Incident Reporting

Monthly reporting in Archer will begin with the January report in February 2015. The final monthly report will be submitted through SIRS for the December report. SIRS will be disabled in February 2015. Historical information is available on the DIR website and summary incident reports in the TX-ISAC Portal. All security incidents submitted during the prior month in the Archer system will roll up into the agency's monthly record. Agencies can add additional incident occurrence information to get a total records for the month. Monthly Incident Reporting has been streamlined to minimize effort while gathering important details.

What You Need to Do to Prepare

Information Security Officers are asked to respond to the DIR email requesting contacts and permissions by December 8, 2014. Agencies and Higher Education Institutions were asked to provide a list of staff, with email addresses, who will need Create, Read, and Update permissions and who will need read only permission to each of the Incident and Monthly Incident modules. If a response is not received, DIR will provide CRU permission for Incident Reporting to the Information Security Officer, and CRU permission for the Monthly Incident module to current SIRS users.

Users should attend the online training class for working in Archer, reporting security incidents, and monthly incident reporting. Web-based training sessions will be available at the end of December and throughout January. DIR will also conduct webinars during January to preview the system and answer questions.

Users will receive their credentials via email when they are added to the system. This should happen the last week of December.

For further information or if you have questions, please contact us at DIRSecurity@dir.texas.gov

Texas InfoSec Academy

Updates

New Security Course Available

The Certified Information Systems Security Officer (CISSO) course is now available in the Texas InfoSec Academy LMS. Please note that you must complete the prerequisite course work & pass the associated exam(s) for the track you are following before you can enroll in the CISSO course. For all tracks, this includes the CSS course & exam and for the Certified Pen Testing & Hacking track, you must also complete the CVA course & pass the associated exam. Refer to the Texas InfoSec Academy curriculum for tracks & associated courses.

Texas InfoSec Academy Forum

The Texas InfoSec Academy Forum is an online tool for you to use to post course questions, browse topics and participate in course discussions. You can navigate to the Texas InfoSec Academy Forum by clicking on your course on the Texas InfoSec Academy LMS home page and then clicking the Texas InfoSec Academy Forum link.

Instructor Led Sessions

Each Friday, from 1:00 PM to 3:00 PM, there is an online instructor led session in which you can participate. The instructor will review specific course material, lead discussions and address questions. This is a great opportunity for you to enrich your learning experience. All sessions are recorded. You can access the previously recorded sessions on the InfoSec Academy Forum by clicking the link on the InfoSec Academy Forum page. Note: There will be no sessions on December 26, 2014 or January 2, 2015. To find out

Exam Vouchers

Exams are not administered according to any set schedule, instead, you can request an exam voucher and sign up to take an exam when you feel you are ready. You must score a 70% on the exam in order to pass it and have two opportunities (by using a voucher) to pass an exam. If you've exhausted your opportunities and have not scored a 70%, then there will be exam fees associated with future attempts. Contact Michele Elledge at infosecacademy@dir.texas.gov for an exam voucher.

Questions?

If you have any questions about the Texas InfoSec Academy, you can send an email to infosecacademy@dir.texas.gov or call Michele Elledge at 512-475-0419.

Are you using
Gartner Research
today?

Gartner delivers
technology
research to global
technology
business leaders
to make informed

Network Security Operations Center (NSOC) Updates

NSOC – Network Security Operations

The NSOC is producing our first annual threat report for publication in early 2015. This report is one of the many efforts to provide a “Best in Class” Security Operations Center (SOC). Our core capabilities at the NSOC are detection, communication, mitigation, and prediction. Currently, we are working to improve our people, processes and technology that we use to support these capabilities. This will ensure we continue to provide the type of service to our customers and stakeholders that provides real value. It is not news to anyone at this point that numerous public and private entities are experiencing breaches at an unprecedented rate. Why is this? The greatest achievement of the modern age is our ability to network and connect to each other through technology. This also means that our information is increasingly available to those who would seek to steal it.

For a long time the mantra in network defense had been Defense in Depth. This methodology has been effective for a time and is based on the principle of defending a castle. This no longer works as the principle strategy. The bad guys trying to attack the castle are effectively flying jets over the wall and dropping weapons from above. So what do you do to fight nefarious characters who are out there and have improved capabilities to avoid detection? Nationally, the typical time it takes a breached organization to have detected the breach after it occurs is over 200 days.



Current, efforts at the NSOC are centered around ensuring that we are doing everything we can to shorten this window as much as possible. Other themes that emerge are that bad actors will still try the path of least resistance despite sophisticated attacks, un-patched systems, poor change management,

improper asset inventory and control procedures continue to be exploited. Through the DIR NSOC’s involvement in evaluating new and emerging security technologies, we strive to remain a leader in partnering with the best minds in the security business. Through these partnerships we are better equipped to deliver true value to the State of Texas.

Information Security Officer Spotlight

Sean Miller Information Security Officer Railroad Commission

I began working with the state at the Texas Department of Protective and Regulatory Services as the Registrar, and then progressed to working at the Texas Youth Commission, holding several positions. Initially, I was the Director of Data Management for Education, later becoming the Director of Operations. After which I moved to the Texas Commission on Environmental Quality as a Section Manager and then to the Railroad Commission of Texas as the Program Manager and Information Security Officer.

How did you come to the security field?

Security has been an interest of mine for many years. Working with the students at the TYC was always a challenge as we delivered educational, health and administrative services to a population that was curious and fearless while maintaining administrative systems to provide services. After which at TCEQ I maintained interest and for a time managed information security. I was then fortunate enough to be offered a position at the RRC as the ISO.

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

Information security is constantly evolving. Initially it revolved around preventing unwanted access or attacks, then focus shifted to securing access to systems, then refocused to data and classification of data, then onto the next topic and so forth. Security seemed to be stuck in a "whack a mole" cycle with focus being technological solutions that were added on as an afterthought. This approach evolved over time as organizations have learned that the "whack a mole" approach was not only costly and impractical to maintain, but left them open to unmanaged risks.

Today's management of security requires a shift in thinking and planning to address the risk to organizational business practices as a whole. Long term and short range planning integrated within agency business outcomes are becoming an important aspect to implementing sound security methodologies.

Additionally, organizations are recognizing they need to protect themselves from internal and external threats by offering education services, updated policies and procedures, adherence to sound software development methodologies, as well as the implementation of traditional technological solutions.



As the state's Information Security representatives, we must also continue to adapt to newer solutions and recognize that we support the business functions and the users. To this end, we must also continue to educate ourselves not only on technological solutions, but also on risk exposure created by legal obligations related to hosted services and advanced computing technologies. We must also establish baseline metrics based on the success of business outcomes to measure progress rather than the metrics based on traditional usage reporting, and through developing effective relationships with our business partners. This will help us be viewed as value added, rather than burdensome.

In short many things have changed over my career, but the most drastic has been the recognition by agencies that security cannot be provided solely through technology, but rather through the management of risk based on business needs.

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

Our users/customers are internal staff, contractors, regulated community and the general public of which our business partners in each division are the most challenging. We work extremely hard to educate and partner even closer with them to provide solutions which meet the needs of the agency while maintaining an adequate security posture.

How did you first learn about Rail Road Commission?

I have been aware of the Railroad Commission for many years but only learned of its great history since I have been employed here.

What do you like best of your job?

The best part of this position is the opportunity to work with and learn from our diverse business partners in the commission to

develop IT solutions which help service the regulated community, who create jobs and service the public as a whole.

What would people never guess you do in your role?

Spend countless hours reviewing Government and Administrative Code.

What other career would you have liked to pursue?

If I had any choice, I would love to work in the Park Service as a photographer or assist with park management.

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

The greatest professional challenge I have faced to date continues to be establishing a sense of urgency without creating a sense of disorder. To accomplish this I work continually with a great team to resolve issues and remain committed to procedure.

Tell us about your most proud accomplishment.

I am fortunate to work with a great team; building that team has been great achievement but mostly I am proud of their accomplishments as a team.

Top 3 life highlights.

Marrying my wife
Daily enjoyment of my three children
Freedom to experience the Texas Parks and people.

Where did you grow up?

Globally

Do you have family in Austin?

Just my immediate family (Wife and 3 children)

What are your hobbies?

Photography and Smoking BBQ

People would be surprised to know that you...

Like to play "cook" with my daughter.

Any favorite line from a movie (Song Lyric)?

"You've got to accentuate the positive
eliminate the negative
Latch on to the affirmative" Sam Cooke

Are you messy or organized?

Somewhere in between.

Favorite travel spot?

Big Bend

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

World War Z

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

Pink Floyd – The Endless River

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

Pope John Paul

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

Brisket Breakfast Tacos

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

Alfred Stieglitz

Least favorite food?

Chicken Liver

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

The Great Messy Adventure

Describe what you were like at age 10.

Nerdy and loved the outdoors

What is one thing you couldn't live without?

Friendship

What is your hidden talent?

Reading personalities

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

Don't forget the three D's: Dedication, Determination and Devotion leads to success

What would be your advice for a new security professional?

Learn from your partners to balance security implementation with business objectives.

Rail Road Commission

The Railroad Commission of Texas was established in 1891 under a constitutional and legislative mandate to prevent discrimination in railroad charges and establish reasonable tariffs. It is the oldest regulatory agency in the state and one of the oldest of its kind in the nation.

Insight from our Texas CISO

On this day before Thanksgiving there are several things that are on my mind. Writing an Insight article for the December issue means that you won't see this until after the holiday, and my original thoughts were both retrospective and looking forward to next year. So bear with me as I share some thankful thoughts, some reflective thoughts, and some forward looking thoughts with you.

DIR is in the middle of a significant update to our website, and I am excited to see how things are shaping up. The sessions we have had to update the content in the security section of the site have provided us an opportunity to really evaluate all of the progress that we have made in the OCISO this year. So before I get retrospective, I really want to praise my team and say how thankful I am to work with such an elite group of information security professionals. I am truly blessed to get to see the profound impact they are having in the Statewide Security Program.

Ted James has been a steady presence in the group, supporting our customers through the introduction of new services and change throughout the year, and with much more to come, we know we can rely on him to be there to help you.

Claudia Escobar has raised the bar and met new challenges in every aspect of the services we are providing and planning. Her expectations for perfection truly bring out the best in all we do, and I am very happy that she has brought her experience and expertise to our ISO community. The Texas InfoSec Academy that she has designed is truly a remarkable program. I know I can count on her to take on our next challenge in coordinating cybersecurity efforts across the state.

Nancy Rainosek set my expectations for her at high level when I worked with her at HHSC, and she continues to exceed. The Governance, Risk and Compliance solution she is building is an absolute game changer. When she has finished leading the effort that enables us to instrument the security programs across the state, Texas' ability to manage risk will be among the leaders within the security industry. Nancy's willingness to step up and take on anything the program needs help in is a testament to her servant heart.

Jeff Rogers has been a stellar addition to our team. Security within the Data Center Services is rapidly gaining ground, and his experience and exceptional knowledge is not only integrating our statewide program in the DCS arena, but improving the statewide program at the same time. I am excited to see how the merger of these aspects evolves in the future, and how Jeff will take us to another level.

We have two members joining our team this month as well. Hannah Folgate, who has been onboard in a part time role since this summer will be taking on a broader role in helping us communicate clearly and effectively with our customers through this extremely dynamic time. Her delightful personality is cleverly wrapped around a tenacious nature that makes her fearless and capable of everything we put in front of her. And by the time this newsletter hits the streets, Suzi Hilliard will have come on board to spearhead the delivery of our service offerings. We look forward to gaining her perspectives as she comes to us from the Office of Attorney General's Child Support Division, bringing yet another experienced state agency security professional to the team.

Lastly, I am extremely thankful to have the opportunity to work with Eddie Block every day. His intellect challenges me to be better, his capabilities in every area allow our group to accomplish everything my crazy brain comes up with, and his spirit makes it a joy to serve in this Great State of Texas, because he drives us to be our best. He is not only my right hand, but a friend that I know I can count on.



*Brian Engle
CISO, State of Texas*

Any leader would be envious to get to work with the team that I have been blessed with, but it gets even better. The opportunity to collaborate with an incredible group of Information Security Officers throughout the state, with groups like our Statewide Information Security Advisory Committee and all of the subcommittees, the Information Security Working Group, the Statewide Security Operations teams as well as the Network Security Operations Center team, our Controlled Penetration Testing Team, as well as all of our partners. Thankful does not say enough.

In retrospect, this past year has given us the opportunity to develop the Texas Cybersecurity Framework, a collective effort that many of you were pivotal in producing. With a revised TAC 202 soon to be published, an Agency Security Plan process that will put security programs across the state on a roadmap of continual and steady improvement, and an eGRC solution that enables us to manage the Framework's elements while relating our maturity to risk, and a cyclical management plan that keeps all of the components on track for evolution into the future I am confident that we are well suited to manage risk within the state at a highly competent level.

With a content rich and comprehensive Texas InfoSec Academy established we not only have a platform to provide our Information Security Officers the knowledge they need to be a well-rounded CISOs of the future, we have the ability to educate IT personnel to prepare them to provide depth in our ranks. And finally, although a number of other items have been left off of this list, we have seen a transformation in our DIR Cybersecurity Insights newsletter that you are now reading, which has even more improvements to come.

I am thankful that you have stuck with me this far in what is a longer than usual article, and thankful for all that you do to serve the citizens of our state by protecting information resources within your organizations. My thoughts to our future now turn towards the 2015-2020 strategy that I am currently constructing, and I look forward to sharing insights of that strategy with you in the upcoming months. In the meantime, be safe and joyous throughout the upcoming holiday season. Pause from this forward looking time of leadership change, upcoming legislative session, budget preparation or other tasks of tomorrow to take time to enjoy time with your families and your teams, and consider what you are thankful for as you reflect on all that you have done this year.

Brian Engle

Events

DIR participation in Cybersecurity Events

- Eddie Block, Deputy State CISO and Claudia Escobar, Security Program Manager served as judges for a Computer Fraud research and presentation of an MPA class at The University of Texas.
Date: First week of December, 2014
Location: The University of Texas. McCombs School of Business
www.dhs.gov/ccubedvp

Training and Conferences Around the State

Monthly Security Program Webinar

How to Achieve Success With Cyber Risk Assessment and Analysis

Date: Tuesday, December 9th, 2014

Time: 2:00 pm CDT

<https://www1.gotomeeting.com/register/429716433>

TASSCC State of the State

Date: Friday, December 12th, 2014

Location: Hyatt Regency on Town Lake

<http://www.tasscc.org/>



Feedback, comments, stories, etc.

DIRSecurity@dir.texas.gov



Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas