

THE DIR CYBERSECURITY INSIGHT

January FY2016 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV



Tools for the Resolution

We are almost halfway into the month of January (already!), and there have been several (dozen) resolutions made and broken. That gym membership and 5-day/week workout plan? Oops. That diet we started? I'll start it over on Monday. The resolution to be a nicer person? That worked until the day that everything went wrong.

Although our resolutions don't always last as long as we planned, the intention is good. The notion of improving ourselves can easily translate into the security world. As security professionals, we are always striving to improve awareness and become stewards for our vocation.

DIR also strives to enable you on this mission, and offers several tools to help. Some of these tools are described below. For additional information on any of these products or services, please contact DIRSecurity@dir.texas.gov.

Security Awareness – SANS Securing the Human

DIR has purchased licenses of SANS Securing the Human Security Awareness training. This training consists of video vignettes focused on single topics. The videos are no longer than 5 minutes in length, and can be used as a tool in your organization's security awareness program. SANS runs the training on their own Virtual Learning Environment (VLE); however, you can pay a small fee to integrate the training into your own LMS.

Security Assessments – Controlled Penetration Tests and Organizational Assessments

DIR continues to offer Controlled Penetration Testing, Vulnerability Assessments, and Web Application Vulnerability Scans for free to state agencies and institutions of higher education. The type of vulnerability tests vary, based on your organization's needs. Our scan team uses a combination of automated tools along with manual testing to provide comprehensive results regarding your network and application vulnerabilities. In addition, DIR will continue to offer Organizational Security Assessments (contract still under negotiation), which gauge the overall security 'health' of the organization.

CONTENTS

Monthly Article

Tools for the Resolution **P.1-2**

NSOC Update

Information Notifications **P.2**

Our State ISO

Spotlight

Jon Tidwell **P.3**

OCISO Corner

Nathan Goggin **P.4**

From our State

CISO **p.5**

Events **p.6**

The state entity will receive a list of strengths and weaknesses for management, along with a roadmap and suggested plans to improve the security posture of the organization.

Incident and Risk Management – Archer GRC Portal and Tabletop Exercises

The Archer Governance, Risk, and Compliance (GRC) Incident Reporting Portal addresses security incident and event reporting requirements for state agencies and institutions of higher education. The Archer GRC application provides advanced incident management capabilities and analysis, along with the ability to conduct risk assessments.

DIR offers tabletop security exercises in partnership with the University of Texas at San Antonio's Center for Infrastructure Assurance and Security (CIAS). These exercises can help state entities prepare for various event scenarios to ensure you work through any kinks in your incident response plan/procedures and fix major issues BEFORE a real incident happens. Tabletop exercises can be found [here](#).

Collaboration and Education – Security Workgroups, InfoSec Academy, Monthly Webinars

DIR facilitates the Information Security Working Group (ISWG), which meets on a monthly basis. In addition, there are mailing lists available to discuss ideas and issues with other security professionals. A description of these mailing lists and links to sign up can be found [here](#).

The InfoSec Academy (contract still under negotiation) was established to provide a path to valuable security certifications to Information Security Officers and security analysts for the state of Texas.

DIR will continue to provide tools and help you and your organization be more secure in this New Year. That's not a resolution – that's a commitment to you. Please reach out to us if you have any questions, or would like information on security services that DIR offers.

Network Security Operations Center (NSOC)

Since February 2015, the DIR NSOC team has been adding security alerts into the Archer incidents application. Agencies have been very quick to respond and acknowledge these time sensitive alerts. This process has enabled improvements for agencies, the NSOC Security Team, and quality tuning of the NSOC security tools. We appreciate your support in this endeavor.

The NSOC Security team also receives other types of security information from a diverse set of sources that may not rise to the level of a standard NSOC alert. For example, alerts for smartphones on the State network which are most likely personal devices or alerts from a public Wi-Fi network. Normally, these alerts would be deemed un-actionable and we would not send you an alert on this activity.

Going forward, the NSOC team will begin sending these un-actionable alerts with the title "Informational Notification". They will be entered into the Archer incident application like our actionable alerts to permit tracking and reporting. The NSOC team will not expect quick action or feedback on Informational Notifications. These notifications will be tracked differently than our standard NSOC security alert. If for some reason the notification elevates to the level of an actual incident, you can mark the incident as "confirmed" and continue to work the incident in Archer.

Please email security-alerts@nsoc.dir.texas.gov with any concerns or questions.

Information Security Officer Spotlight



Jon Tidwell
Information Security Officer, CISSP, CCNA, CCSA, ITIL
Government of Collin County

I have a BBA in Management Information Systems from Dallas Baptist University. I was a 'working student' graduating from college 11 years after high school. I wouldn't recommend this path to everyone (especially my kids) but I would not change a thing about my path to the degree.

I'm a recovering Air Force Brat, son of an OSI computer crime investigator. I'm quite fortunate that my wife (finally) agreed to marry 16 years ago. We have four kids and live in Little Elm, Texas. I'm doing my best to help my kids understand 'how' the technology they use actually works. For Christmas my older boys received a Python programming book and lock pick set.

I am the first IT Security Officer for the Government of Collin County. We are the county just north of Dallas, and are one of the fastest growing counties in the nation, slated to have our population surpass 1,000,000 people in early 2016. I have been in this new seat for almost a year now, working through a long term plan to improve our position across the 20 Critical Security Controls.

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

When I first started in security, it seemed we focused on the perimeter, physical security and more firewalls. Also, a security incident was an 'IT Problem', an impression of us not doing our jobs correctly. Today, the evolution of the hacker increasing the attack surface of a target entity has us thinking about security in everything we do, everything in the castle, not just the walls. Also, I think the impressions of

breaches are changing, that they are business problems, not just IT problems.

What do you like best about your job?

My team. The growth of our County, has allowed us to be in a fortunate spot, to actually have a 'security team' even if it is myself and Michael, but he has a passion for this space and shares my desire to be a national leader. It's fun and motivating to be around that kind of fervor every day.

Top 3 life highlights?

- Attending Andrew Jackson Middle School in Forestville, Maryland. My two years at that school taught me more about interacting with people than any other time in my life.
- Living in Kaiserslautern, Germany. Great town, great people, great memories.
- Marriage, from day one to now. I know it's a standard answer, but it makes me who I am.

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

Sequoyah. Being of Cherokee descent, his story has always fascinated me and I'd love to pick the brain of a person that can create an alphabet from a spoken language.

What would be your advice for a new security professional?

First, a security professional should be an enabler, integrating with business processes, not stopping them. Second, understand the process... whatever it is, from beginning to end, because your adversaries do. Last, GSEC before CISSP. Yeah, I said it.

OCISO Corner – Getting to Know the Team



Nathan Goggin
Information Security Analyst
Department of Information Recourses

What is your responsibility in DIR and with the State?

My primary duties are to coordinate and facilitate the Controlled Penetration Test process for state agencies and to assist in the distribution and administration of cybersecurity material to agency users.

When and where did you start your career?

I started my IT career back in my early 20s, building PC systems for friends while attending New Mexico State University (NMSU). Since jobs were scarce in the southwest, I had to take what work I could find after college. I started out as tech support for a local ISP and eventually worked up to system administration with a contractor for Apple. My background finally provided me an incredible opportunity as a systems analyst with the State of Texas.

Why the security field?

Information Security was a fascinating subject in school, but it was also the one most overlooked. I enjoyed learning about cryptography, digital forensics and the manipulation of technology.

As a system administrator, I knew that securing systems and educating users was key to keeping our technical environment safe. It wasn't until I witnessed the social-media world start to take notice of DDoS attacks, corporate hacking and the release of PII that I realized the need of a firm understanding of information security. It wasn't enough for me to inform a user on HOW information security worked but WHY security measures are so important.

We live in such a digital age, that security can often be taken for granted. I've seen, first-hand, how the exploitation of PII

can affect a person. I chose the security field because I wanted to have at least some capability of minimizing the negative effects unethical hackers have on innocent users and organizations.

What did you think you were going to be when you grew up?

I loved math in school so I thought: engineer. My dad thought: accountant. Fortunately, we were both wrong.

What is the greatest lesson you have learned?

For me, two lessons are tied for greatest. 1) It's never too late to find the courage to be yourself. 2) No one knows what they're doing. Deep down, everyone is just faking it until they figure it out. –April Ludgate (Parks & Rec)

What do you want your legacy to be?

I don't know if I believe in leaving a legacy. People should make their own way in their life and career. If there's anything anyone can learn from me it's that you should never stop learning or being an open-minded person.

Do you have a favorite hobby or pastime?

I enjoy hiking, kayaking, off-roading, gaming, electronics tinkering, trying DIY projects at home and playing with my kids. I may not be good at them all, but my enthusiasm holds true.

What do you like best about working at DIR?

I like the overall work environment very much. The staff here is friendly and willing to assist me when I have questions. My team has been especially welcoming and patient.

Insight from our Texas CISO

CISO Extended

As the CISO for the state of Texas I rightly focus most of my attention on the statewide security, policy, and boundaries of the statewide network. Too narrow a focus, however, can blind us to the bigger picture. To that end, over the past few months, I've spent a lot of time outside of the office and state of Texas. I traveled to Salt Lake for the NASCIO Annual Conference, to San Diego for the MS-ISAC annual meeting, and spent several days observing a statewide cybersecurity exercise in Arizona. Speaking to other state CISOs and seeing the work that other states are doing is enlightening, reassuring, and motivating.

I'm pleased to report that Texas is leading the way in several areas. The Pell Center for International Relations and Public Policy recently identified Texas as one of the top state cybersecurity programs¹. Highlighting the NSA/DHS Centers of Academic Excellence in our state universities, the GRC system that DIR is building, and the work of our advisory councils, Texas has a strong framework from which to build a leading cybersecurity environment.

Discussing other state's programs with their CISOs confirmed that there are challenges we all face regardless of state size, governmental structure, or executive involvement. As we've seen in Texas, finding security professionals is not an easy task. This is a shared feeling across the country, there just don't seem to be enough people to fill all the positions we need. Most states also struggle to "sell" the security story in a way that non-technical staff, both front-line and executive, can buy into. This can lead to people ignoring policy, inadequate funding, or prioritizing new services over secure services. There is some level of comfort in knowing we are not alone and the sharing of ideas helps us all.

It is also interesting to see the areas of security upon which other states focus. I traveled to Arizona to observe a two-day statewide cybersecurity exercise in hopes that Texas can host a similar statewide exercise. The first day was primarily focused on the private sector response, with day two focusing on the public sector. I wanted to see how they ran their exercise and take some lessons from their successes and challenges. What impressed me most was the relationships and cooperation between the public and private sector. Mike Lettman, the Arizona CISO, has spent much of his time building connections within his state and it showed. I have a lot of work to do in this area and the trip proved a strong motivator. By the end of the visit my questions were less about the exercise and more about the relationships.

So, as we enter a new year, it is a good time to take inventory of the successes and failures of the previous year and to set goals. With the first parts of the GRC program, a revised and renewed TAC 202, and more legislative focus, we are pointed in the right direction. There has been substantial growth in the past year but there is no finish line in security and we must continue to build, adapt, and evolve.



Eddie Block
CISO, State of Texas

Eddie Block
CISO, State of Texas

¹ <http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/>

Events

2015 Save the Dates

- General Land Office Sponsored CISSP Boot Camp Feb 22- 26 2016
 - Instructor: Doug Landoll
 - \$1750.00
 - Contact: Brandon Rogers 512-463-5763
- Information Security Forum: April 14-15

OCISO Participation Around the State

- Eddie Block, Claudia Escobar and Jeff Rogers attended TASSCC State of the State held December 11.
- Eddie Block and Claudia Escobar participated in the Arizona Statewide Cybersecurity Exercise held December 8-9.