



DIR Cybersecurity Insight Newsletter

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

Power on 2015!



Contents

Monthly Article

Starting 2015 prepared 2

Texas Information Security Program Updates

Incident Response and
InfoSec Academy 3

Network Security Operations Center Update 4

Our State ISO Spotlight

Amar Yousif 5, 6, 7

From our State CISO

2014 8

Events 9

Starting the Cybersecurity Year with the Right Foot

With 2014 in the rearview mirror, it is fun to look forward to the year ahead and see if we can predict what may happen over the next twelve months.

Cyber Security Experts begin to make their predictions.

“While no one can totally reliably predict the future, there are often good indications in what we see that provide likely directions for the coming year,” says Geoff Webb, Senior Director, Security Strategy with [NetIQ](#). “For example, it was pretty clear at the end of last year, after the details of the [Target](#) breach became public, that it wasn’t going to be a one-off incident. Rather, it was the opening salvo in what has proven to be a year-long attack on the retail industry.”

Attacks against virtual payment systems

“We expect to see cybercriminals focus more on new payment systems as they are adopted and the potential for criminal financial gain thus increases. This will be in the shape of attacks against banks/virtual currency operators, the end users and their devices, and everything in-between. In fact, we already have some examples of malware stealing virtual wallets from users’ devices and very high-profile incidents of banks themselves being infiltrated,” Patrick Nielsen, Senior Security Research with [Kaspersky Lab](#).

Data Loss Prevention (DLP) broadens its capabilities

Machine learning, pattern recognition and ‘post-send’ message controls are the next wave of DLP functionality that will protect employees, clients and increasingly the brand, according to Cameron Burke, SVP of Business Development for [Cirius](#).

Raw security incidents will continue to rise

The recent Sony attack is a warning of just how devastating a cybersecurity incident can be and that we need to be prepared for just about anything. As Sungard AS’s Director Matthew Goche states, “There are more bad actors who are more organized with better tools and have more upside than ever before. This trend does not show signs of subsiding. Our internal data gathering shows a significant increase in cyber events.”

Thinking beyond individual threats

“Focusing on the individual threat is a common approach to IT security; however, this doesn’t work in today’s threat environment,” Stephen Pao, GM Security at [Barracuda](#), points out. “With the move to virtualization, the cloud, and the mobile internet, the attack surface is expanding. Organizations must make that shift as well to cover all areas of exposure – email, web applications, remote access, web browsing, mobile Internet, and network perimeters.”

All these security predictions can be come true, or at least in part. The question is, are you prepared?

Program Updates

RSA Archer GRC Update

The RSA Archer Governance, Risk, and Compliance (GRC) system is now live!

The RSA Archer GRC system will initially be used within the state of Texas to address the responsibility of the organization under TAC 202 to report security incidents. The system will enable you to complete incident reports, will automatically notify DIR OCISO of urgent incidents, and will automatically generate monthly incident summary reports that include all confirmed incidents for your organization in the previous month.

Organizations can record more than urgent incidents in the system, giving them a central point for recording all security incidents.

All incidents entered into Archer by an organization for a given month will be compiled to form their monthly incident summary report (formerly reported via SIRS), which is also required to be reported to DIR. The more information entered into GRC System, the less additional information you will have to add to complete your monthly report.

Upcoming changes to TAC 202 require organizations to report urgent incidents and a monthly summary in a form and manner specified by DIR. Archer is DIR's specified method for reporting urgent incidents and the monthly incident summary. You may still call or email DIR with your urgent incident information, DIR will then input this into the system so you can update the urgent incident report as you work through the incident response process.

All ISOs and organization's incident contacts should have received an email with instructions on how to gain access to the system and where to get training. You can download an e-learning class at:

<http://www.dir.texas.gov/security/operations/Pages/incidentreporting.aspx>.

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

Texas InfoSec Academy

The InfoSec Academy is starting the year off with a new round of instructor-led sessions for the Certified Security Sentinel (CSS) and Certified Vulnerability Assessor (CVA) courses. In addition, the InfoSec Academy will introduce the first instructor-led session of the Certified Information Systems Security Officer (CISSO) course. Online sessions are held every Friday from 1:00 to 3:00 PM CST and are recorded. If you were not able to start courses when they were first offered in November, this is a great opportunity to start these courses now.

Before taking the CISSO course, you must first pass the fundamental certification exam for the track which you are pursuing. The CSS is required for all tracks; the CVA is an additional requirement for the Pen Testing & Hacking track. You may place out of the CSS and CVA courses by passing the exam. If you would like to take one or both exams and need an exam voucher, please email infosecacademy@dir.texas.gov.

[Click here for more information about the InfoSec Academy course tracks.](#)

InfoSec Academy login:

<https://infosecacademy.dir.texas.gov/>

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

Network Security Operations Center (NSOC) Updates



The Network Security Operations Center (NSOC) will publish its first Annual Threat Report during the first quarter of 2015 as part of an ongoing effort to increase our communications and to provide an update on the activity we have seen over the past year. In this report, the current security posture of the state's shared network will be discussed as well as the NSOC's goals achieved in 2014.

We also want to define who we are and what we do. The NSOC is a component of the state's overall security plan that includes the DIR OCISO, State of Texas DCS, and most importantly our customer's security programs. After reading the report, it will be clearer how the NSOC fits into that model. Other topics include lessons learned, vendor research, trends, and emerging threats.

Throughout 2014, the NSOC has continuously fought alongside our customers to prevent infections. We have blocked brute force attacks, mitigated several Denial-of-Service and Distributed Denial-of-Service attacks, and vigilantly monitored the network for malware. Another significant event was the network upgrade to 10G capacity with full redundancy. This move was accompanied by similar upgrades to our security sensors to handle the additional required capacity.

We have assessed our own capabilities and found many areas that presented us the opportunity for growth and development. Our mission essential capabilities are communication, detection, mitigation, and prevention. We measure our capabilities through the people, processes, and technology that support the capabilities.

The IT security sector has many products and services capable of defending Texas' shared network. These tools and services are continually evaluated to determine if they provide value to the NSOC and its customers. With all these changes and with the Legislative session coming up in 2015, we believe it is in the state's best interest to provide this summary report to anyone familiar with our operation but also for those that might not be familiar but are interested.

If you have questions on anything covered here or questions regarding the NSOC in general, please contact Jeremy Wilson, SOC Manager, at Jeremy.wilson@dir.texas.gov.



Jeremy A. Wilson

DIR Security Operations Center Manager

Information Security Officer Spotlight

Amar Yousif, CISSP, C|CISO, GIAC certs
Chief Information Security Officer
University of Texas, Health Science Center at
Houston

Bachelor of Science in Electrical Engineering from the University of Baghdad 1997.

MBA from WGU of Texas 2013.

Currently working on an Advanced Computer Security Certificate from Stanford University. Expected completion date is 2015.



I started my career in Dubai, UAE, immediately after graduating engineering school. I was fortunate enough to be given the task of starting an IT department from scratch in a multinational manufacturing company. I designed the IT infrastructure, hired staff, and managed vendors to stand up the company's first ERP system. I then moved to Houston to run the IT infrastructure – to include security and regulatory compliance – of a midmarket oil and gas services company. The job took me many places around the world and allowed me to expand my knowledge and expertise in the information security area. I then started my career with UTHealth at Houston and have been there for almost 8 years as the Chief Information Security Officer.

How did you come to the security field?

I was put in charge of organizing the IT environment to deliver SOX section 404 compliance in 2004. Designing, implementing, and then testing security controls over all sorts of IT systems was a big component of that role. I worked with auditors and security professionals to bring the IT environment into compliance, and I became a security guru in the process.

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

The profession of information security has matured from merely running such security tools as the firewalls and the anti-virus systems to becoming an integrated component of risk management, compliance, and IT operations. Properly running firewalls and other security tools is still a pillar of a good information security department. However, designing non-porous systems and helping business managers erect secure processes – not just systems – are now also within the scope of a solid information security function.

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

IT system consumers, business managers, and IT professionals are the main three categories of users whom I help. Each category requires a unique approach and it comes with its own challenges.

Security needs to be frictionless and 'baked in' for it to be effective for consumers. That is a big challenge.

Business managers need to understand the liability they are taking on by going to production with less than secure systems or processes. The challenge of the CISO is to quantify that liability and then help tweak the system or the process by introducing practical security controls so that liability is minimized.

IT professionals are the folks who run most security functions. The goal should be to educate and train them so that they are qualified and aware of the reasoning behind the security work that they need to carry out. The CISO should solicit feedback and listen to advice from this category because IT professionals are usually on the front lines of the cyber battle and are closer to emerging threats.

How did you learn about UTHealth?

In 2007 I was looking for an organization that would keep me in Houston and require less travel. UTHealth attracted me because of the diversity of opportunities and challenges it offered. UTHealth is a not-for-profit organization with a public mission to serve the community.



Therefore, I knew that the work that I would do at UTHealth would positively impact the Houston community, educate the future leaders of healthcare, and facilitate groundbreaking discoveries in healthcare.

What do you like best of your job?

I enjoy that the work environment at UTHealth is vibrant and never boring because of the broad range of education, research, and healthcare related activities that are always happening on campus. UTHealth is multidimensional; it's a university, a research center, a physician practice, and a hospital all rolled into one. Therefore, I get exposure to a multitude of industries. The experience and the professional satisfaction I gained at UTHealth are unmatched.

What would people never guess you do in your role?

The job involves a fair amount of selling of ideas to a diverse group of stakeholders. I do a whole lot of listening to understand what my constituents are looking for and then I do even more talking in order to sell them ideas to help them adopt more secure processes and systems.

The CISO job may have some authority to decree certain initiatives, but it is much more effective to do more selling and less decreeing.

What other career would you have liked to pursue?

I grew up wanting to be an astronaut, and I would still do it if I am given the chance!

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

I faced many challenges over the course of my 18 year career. One of the greatest involved learning how to become a better leader of people. Leadership is about

influencing and inspiring, not controlling and micromanaging.

Tell us about your most proud accomplishment.

I am a proud father of two smart, strong, and beautiful daughters. They are my most proud accomplishment.

Top 3 life highlights.

- Graduating Engineering School in 1997
- Becoming a father in 2001
- Being naturalized as a US Citizen in 2006

Where did you grow up?

I was born and raised in Baghdad, Iraq. My love affair with technology and engineering started in the mid-eighties at age 13 when I put my hands on my first computer, Aquarius, which I now know was made by Mattel, the same company that brought us the Barbie dolls. I spent many subsequent summers eagerly stretching that 4K RAM computer to its limits saving my programs to cassette tapes while other tweens preferred to play soccer.

Do you have family in Austin?

I have family in Houston, Austin, Chicago, Canada, the Netherlands, and Iraq.

What are your hobbies?

I'm a runner and a lifting enthusiast. I try to make it to the gym three times a week.

People would be surprised to know that you...

I am a fan of poetry and all things that rhyme. Folks will tell you that I recite poetry all the time. Even at work events I feel the need to chime. Sometimes orally; other times with s/mime.

Any favorite line from a movie?

Given the context of this interview, it has got to be the line: "I fight for the users" from Tron.

Are you messy or organized?

Organized, but you wouldn't know it looking at my office.

Favorite travel spot?

Waikiki Beach, Hawaii, in the winter, and Cocoa Beach, Florida in the summer. I love water and sunshine.

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

"Think Like a Freak" by Levitt and Dubner (the Freakonomics podcast guys). It teaches you to question everything and base your conclusions on only evidence and data.

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

Do people still use CDs? I have a long commute. I spend two hours a day in my car. Therefore, I listen to a number of podcasts and audio books such as "Security Now" by Steve Gibson, "Stormcast" by SANS, "This American Life" from WBEZ Chicago, and "GPS" by Fareed Zakaria.

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

My hero, Neil DeGrasse Tyson. He is able to take complex scientific concepts and explain them in easy and fun ways, making science accessible to the masses. He is also passionate about science and math education, a cause that is of great interest to me.

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

Breakfast because it involves eggs. They can be scrambled, sunny side up, over easy, omelet, poached, hard boiled, soft boiled, deviled, and even raw. The number of possibilities and nutritional value are high.

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

Stephen Hawking in order to experience how one can be so restricted in body yet so free and genius in mind.

Least favorite food?

I'm sure okra is a decent vegetable, but I never liked it. I would only eat it if it was well battered and fried.

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

"The Unexpected Life." My life has taken many unexpected turns, and I have come to realize that the only constant in life is change. I have been fortunate that most of the unexpected turns in my life have been positive.

Describe what you were like at age 10.

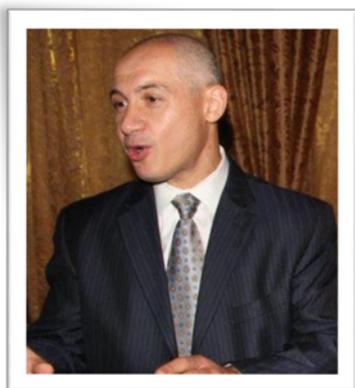
I was a science geek at age 10 and still am at age 40. I spent my free time reading age-appropriate books about the solar system and space in general. My parents supported my habits by getting me any book I wanted.

What is the one thing you couldn't live without?

A purpose. I am fortunate enough to work for an employer with a noble purpose, healthcare research.

What is your hidden talent?

Albeit I am not a big gun enthusiast, I am told that I am a very good shot.



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

Humility will help you connect with and influence people more effectively, the kind of humility that C. S. Lewis described as: "Humility is not thinking less of yourself. It's thinking of yourself less."

What would be your advice for a new security professional?

Standing out isn't as hard as you think. Study up so that you are technically proficient, exercise professional courage often (without being discourteous), ask for and take on tough tasks and challenges, and work long hours.

ABOUT UT HEALTH SCIENCE

About UTHealth

The University of Texas Health Science Center at Houston (UTHealth), the most comprehensive academic health center in the [UT System](#) and the U.S. Gulf Coast region, is home to schools of [biomedical informatics](#), [biomedical sciences](#), [dentistry](#), [medicine](#), [nursing](#) and [public health](#). UTHealth educates more healthcare professionals than any other health-related institution in the State of Texas. Its medical school is the nation's sixth largest. It includes a [psychiatric hospital](#) and a growing network of clinics throughout the region. The university's primary teaching hospitals include [Memorial Hermann-Texas Medical Center](#), [Children's Memorial Hermann Hospital](#) and [Harris Health Lyndon B. Johnson General Hospital](#). Founded in 1972 by the [U.T. System Board of Regents](#), UTHealth's 10,000-plus faculty, staff, students and residents are committed to delivering innovative solutions that advance human health and well-being.

Insight from our Texas CISO

2014 has been called the year of the cybersecurity breach. With a ton of exposure, media coverage, and even a 60 Minutes segment detailing the disclosure of personally identifiable information to a national primetime audience, cybersecurity is getting attention. When mainstream organizations experience incidents, those organizations make the headlines in ways that cause lawyers and marketing departments to cringe. When the incidents affect a lot of people, the attention that is garnered creates agenda items at the board level of discussions. 2015 will likely not see any change in this regard.

So here at the onset of 2015 we are seeing the movie industry jump on the bandwagon. Cybersecurity gone Hollywood isn't something I intend to spend my money on, and if I were to make an early prediction I would say that the latest rendition of "Thor" reprising the character of Zero Cool in the movie "Blackhat" will not set box office records nor cart off the hardware at the Academy Awards. But have you ever thought about who would play you in a movie about a cybersecurity incident in your organization? Would it be a comedic performance by the likes of Jason Bateman, or a serious role played by Tom Cruise, or perhaps a bizarre, slightly dark yet quirky Johnny Depp?

While it is a stretch of the imagination to consider your life during a cybersecurity incident played out on the big screen, a certain role playing does occur as you play out the scenarios that are occurring more and more frequently in the world around us. But consider how you would answer the question, "Could that happen to us?"

In previous issues, we have talked about incident response and table top scenarios; but if you can take advantage of the incidents that have hit the media, you should consider threat modeling. Using these publicized cases to understand how vulnerable your organization might be to the conditions present in those breach cases is a good way to ensure that you aren't just exercising your incident response plan; you're also being proactive in the evaluation of prevention and detection measures. Sure, you might not have the specific data elements, or the same defensive measures, or even the same attacker motives that the victim organizations in those incidents had. But I would venture a guess that if you were to abstract an incident and substitute a variable or two that might relate more directly to you, I am betting that the scenario isn't that farfetched.

There are a variety of ways to construct formal threat models, but a simple way is to lay out the biggest incidents that have become public. Evaluate your risks, consider your defensive measures and detective tools, and determine how you might be impacted. Perhaps together we can construct templates for this modeling here at the beginning of 2015. If you already have something that you would like to share, the DIR OCISO Team would love to help. In the meantime, feel free to banter this concept in the Security Email Forum at security@lists.state.tx.us.

See you at the movies.

Brian Engle



*Brian Engle
CISO, State of Texas*

Events

Training and Conferences Around the State

Monthly Security Program Webinar

Navigating Role Management

Date: Tuesday, January 13th, 2015

Time: 2:00 pm CST

<https://attendee.gotowebinar.com/register/8803618443472383234>

Women in Healthcare Cybersecurity & Compliance Summit

Date: Tuesday, January 20th, 2015

Time: 1:00 – 7:00 pm CST

Place: Norris Conference center

618 Northwest Loop 410

#A100

San Antonio, TX 78216

2015 Save the Dates

- BSides Austin: March 12 – 13
- BSides San Antonio: May 10
- 2015 Information Security Forum : May
- Blackhat USA: August 1 – 6
- BSides Las Vegas: August 5 – 6
- Defcon: August 6 – 9
- LASCON 2015: October 19 – 22



Feedback, comments, stories, etc.

DIRSecurity@dir.texas.gov



Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas