WHAT WAS THE TUKERY HACKER ACCUSED OF?

FOWL PLAY

DIR CYBERSECURITY INSIGHT NEWSLETTER

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

# Face It - Facebook is Not Private

It is November, the holiday season is upon us, and it begins with Thanksgiving dinner. Imagine all the great photos we will capture with our phones. Although it is nice to share our pictures, we need to understand the risk of sharing those pictures over social media so that we can protect our privacy.

## How private is our Facebook?

Did you know that someone can see all the pictures you have been tagged in even if that person is not your friend? This is not hacking. It is a privacy option available in Facebook.

To search for a profile simply enter the name of the person you are searching for in the *search box* 🔍, and visit the profile.

Contents

Monthly Article

Face It. Facebook is Not Private 1-2

Health and Human Services System of Texas Awareness Fair 3-4

NSOC Updates

Some cloud security concerns that you may have not thought about..... 5-6

Our State ISO Spotlight

Eric Mims 7-9

OCISO Corner

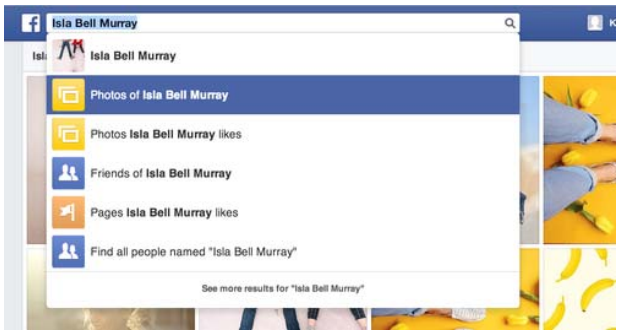
Jeffrey Rogers 9-10

From our State CISO 11

Events 12

For example, let's see how many of Isla Bell Murray's photos we are able to view even if we are not friends (most people at least have a few). Here's the view from her profile page:

Next, let's apply the [Facebook Graph Search](). Simply mouse back to the search field and click once. You'll see a dropdown menu like this:




You can choose from options such as:

Photos liked by "Isla Bell Murray"

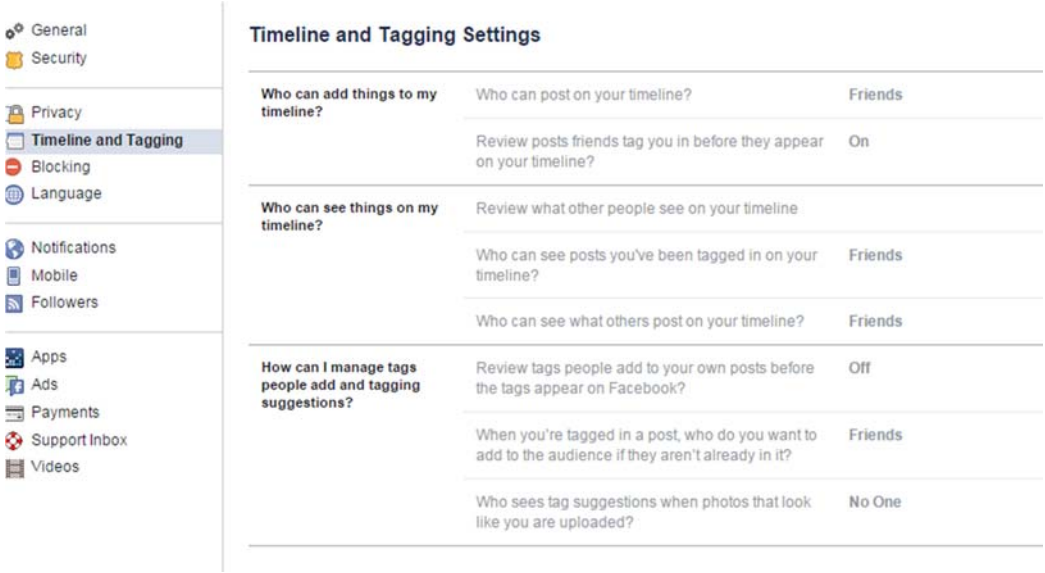
Photos commented on by "Isla Bell Murray"

Now you can see significantly more pictures!

## How can you prevent this?

Under the Timeline and Tagging Privacy Settings, you can set several limitations. For example, you can:

- determine who can post on your timeline
- determine whether you want to review all posts before they appear on your timeline
- determine who can see photos and posts in which you're tagged




Having a social networking presence comes with inherent risk(s). It's best to (re)examine and (re)familiarize yourself with the risk(s), from time to time, so that you can lessen the negative impact(s) to yourself and others. ***Everything clickable… is traceable.***

# Health and Human Services System of Texas Awareness Fair

October was National Cybersecurity Awareness Month. The Health and Human Services' (HHS) Information Security Department grasped this opportunity to raise awareness about the threats and vulnerabilities that can jeopardize the information employees handle every day. The agency held their fourth annual Cybersecurity Fair on October 27th at the Winters Building in Austin. All HHS agencies, including Health and Human Services Commission (HHSC), Department of Aging and Disability Services (DADS), Department of Assistive and Rehabilitation Services (DARS), Department of Family and Protective Services (DFPS), Department of State Health Services (DSHS) as well as external guests were invited. It was a huge success with over 200 people in attendance. The agenda not only held the interest of those who are already passionate about the subject of cybersecurity, it sparked new interest in those who are just becoming aware of how these issues affect them. The goal was to develop a culture where information security is on the minds of even the most casual users of technology in order to prevent employees from becoming targets at home or work. The following topics were covered:

| Speaker Agenda |
|---|
| ***Speaker* – Topic** |
| ***HHS CISO, Shirley Erp*** – The HHS Cybersecurity Program and Battling Cyber Threats |
| ***State CISO, Eddie Block*** – Security issues that people face: phishing, fraudulent websites, and insecure practices |
| ***HHS Chief Privacy Officer, Sheila Stine*** – What Everyone Wants to Know About Privacy |
| ***UT Center for Identity, Katie Stephens*** – Master of Science in Identity Management and Security |
| ***UT Center for Identity, Ryan Anderson*** – IDWise |
| ***Continuity Planners*** – Could you do your job without the Internet? |
| ***FBI*** – Cyber/Counterintelligence Squad Investigating Cyber Intrusions |

In addition to the topics covered in the speaker agenda, the Cybersecurity Fair included booths where participants learned proper cybersecurity behaviors. Posters and other educational material on cybersecurity were also distributed to attendees. HHS teamed up with the University of Texas to disseminate information on the new UT Master of Science degree in Identity Management and Security. Information was also provided about IDWise, UT's online resource, which helps individuals, businesses, and families keep their personal information secure. The fair concluded with tours of HHS Information Security's Cybersecurity Operations Center (CSOC) where IT threats are detected, contained and remediated

A monitor at the Cybersecurity Operations Center shows hacker activity across the globe in real-time.

In her opening remarks, Shirley Erp stated that there are 45 million attempts to hack the Health and Human Services agencies' websites every month and that fighting them off is the responsibility of every employee. "We are a prime target because we have a lot of federal data." Erp said. "That could be very lucrative for a data thief."

Attacks come in a variety of ways; some of the simplest are the most effective. An email telling you to "click here" to verify your account could be nothing more than a phishing scam and once hacking software has embedded itself into your computer, it can branch out deeper into the agency. One of the most effective defenses is awareness of what might be coming, said Eddie Block, the State of Texas Chief Information Security Officer from the Department of Information Resources.

Block said he ran drills where he called employees on a Friday, told them he was from IT and needed three hours of their time on Monday to move their email to a new server. When they complained they didn't have the time to do it, he offered to handle it over the weekend if they'd give him their password. "They always gave it to me," he said. Block said strong passwords and a password manager go a long way to protecting personal data, both at work and at home. He said a good password manager will store different passwords so you won't have to memorize a different one for every site you visit.

The consequences of a breach can be significant. In addition to facing disciplinary action for leaking protected information, a client's/user's life can be thrown into total chaos from a breach. Not only can they suffer financial problems, but their health and well-being could be endangered if a hacker changes critical information within a target's medical records.

Employees need to know when they are dealing with sensitive data and that includes more than health information, said Chief Privacy Officer Sheila Stein. Financial information, social security numbers and even client names can be protected information she said.

Awareness is the key. IT security can't be everywhere. Employees need to recognize when something isn't right, such as an email asking you to click on a link, to provide information, or a letter with the name of a company that's just a little off. Case in point, Block said he received a letter from US Airlines telling him to call for information regarding the free tickets. While there is a US Airways, there is no company called US Airlines.

"We need you to be our eyes and ears," Erp said. "If you think something isn't right, let us know."

## Cybersecurity Tips

- Do not click on links in emails from unknown senders or in online advertising.
- Look for https instead of http (in URLs), especially if you are sharing sensitive information such as credit card numbers. The "s" means the site sends and receives encrypted data which keeps your information secure. Without it, any information including your credit card numbers are there for the taking.
- Be sure to have an up-to-date antivirus and malware detection program on your computer.
- Keep your computer updated with the latest security patches.

# Network Security Operations Center (NSOC)

## Some cloud security concerns that you may have not thought about…..

You can't have a conversation about technology today without the word "cloud" being included. Cloud-based services and applications are being offered to solve almost every business need. There are cloud-based services for a multitude of different functions including file sharing, data storage, email proxies, security gateways, web content proxies, etc. Our state agencies are starting to take advantage of some of these cloud-based offerings and there are many good reasons to use cloud-based services. However, security is always a concern when looking at cloud-based solutions. Some of the most important questions to ask a cloud services vendor are: How will using your service affect my network perimeter security? Will this open a door in my network monitoring perimeter? Can I track users and their actions through the cloud app and my network?

To put these issues into context, allow me to describe a few different scenarios we have encountered at the NSOC.

Agency XYZ is using a cloud-based email proxy service. All of the agency's email is routed through the cloud-based service, both in and out. The vendor then applies security intelligence to all of the email requests and allows those that are deemed as safe to proceed while those that are deemed to be malicious or suspicious are blocked. It can be a great service. In this instance, all the email traffic for that agency passes through perimeter network monitoring tools using just two IP addresses – the cloud-based proxy and the agency email gateway. Without access to logs from both the agency and the vendor, it becomes impossible for the network security tools to determine who downloaded malware when it is finally detected. This is happening today. We will get alerts from our NSOC tools of potential malware delivery (let's say CryptoLocker) via traffic from a cloud proxy to our gateway. At the NSOC, we cannot determine the attacker's IP or location because we show the proxy as the source and the agency gateway as the destination. We can still alert an agency, and if they have the access to their own logs and the proxy logs, they can determine which user was involved and then hopefully remediate. However, if an agency doesn't have that access to logs, all they'll know is malware (CryptoLocker) just landed somewhere on their network. At this point in the process, we now know the cloud vendor has a security gap because it didn't detect and block the malware (CryptoLocker) that the NSOC tools identified. An important point to consider is, how do you communicate these types of threats to your cloud vendor and how quickly do they react to these new threats?

Another issue that you might not think about… cloud vendors use reputation scoring and blocking. If happens to be a cloud-based security service like web content filtering or an email proxy, chances are very high that the vendor blocks access. That is because websites and IPs are given a reputation score. Different vendors use different scoring schemes, but a majority of them use some sort of scoring system. For example, some use a reputation score ranging from 0-100, with 100 being the absolute worst. Other cloud vendors may use a 0-5 range, with 0 as the worst of offenders. From these ranges, a vendor's threshold is set. If a vender uses 0-100 and 100 is bad, security personnel might set their block threshold for anything scored at 80 or above while setting an alert threshold for anything above 60. Whatever the case may be, cloud vendors set thresholds to determine what will be blocked, based off those reputation scores. So now, let's assume a legit website is on a shared-host server in the Congo Cloud but there is also a cyber-gang that has compromised a website belonging to another Congo customer on the same server. All of a sudden, your agency can't access the legit site you need because your cloud vendor is blocking access to that IP address due to its reputation score. How do you get your vendor to grant

your customers access to the legit site when a poor reputation score causes a blockage? What if you host a site on a shared server and your audience can't get to it because security companies are scoring your IP as bad? Both of these scenarios present favorable and unfavorable consequences, so it may be worth asking the vendor how they react to those kind of situations.

One other issue the NSOC has witnessed recently is long delays or web pages timing out when the agency users try to access cloud-based apps. These issues are caused by the routes within the vendor's network cloud. We have noticed two instances where the cloud services vendor was routing our State of Texas user traffic to other continents instead of US data centers. This caused massive application delays and hampered the agency operations. These issues were eventually resolved but they were very difficult to trouble-shoot and required cooperation from the cloud vendors.

Here is something else to consider when working with, and selecting, cloud providers. (This relates to services you receive from the NSOC.) At the NSOC, we gather intelligence from multiple sources, including our own tools, on malicious actors and current threats. We use this intelligence to block traffic to/from any IP address or domain that we believe to be malicious. So when we see an attacker go after an agency, we add the attacker's IPs to our blacklist. Now, all of the state agencies are protected from this threat vector. When agencies use cloud services, we lose a great deal of that intelligence **(and control)**. We can no longer see who is attacking us nor can we determine their location. We may see the malicious activity take place but its source will always be from the cloud proxy and its destination will always be the agency gateway. As a result, we can no longer block specific IPs/domains and agencies will not have the benefit of threat protection from blacklisted sources. This makes it important to consider what types of access, specifically logs, and other pertinent details your cloud vendor provides as it relates to attacks perpetrated through cloud resources.

This is just a few of the issues to consider with cloud-based services and how that may relate to current NSOC services you receive. We are sure there will be more in the future. We just wanted to give you some food for thought as more and more business units look at cloud solutions going forward. Think about your environment and your current security practices and procedures before you meet with cloud vendors. Make sure you ask as many questions as possible, including those mentioned in this article. It may solve some issues before you ever get started.

# Information Security Officer Spotlight

Eric Mims
Information Security Officer
University of Houston - Victoria

My first real job was for the Radio Shack in San Marcos where I discovered I'm not very good at sales. As a student I worked at a number of the computer labs at A&M, finishing with the dedicated computer lab for the College of Education. This got me noticed by some faculty working with a grant and I moved from there after graduation into a technical support/trainer position with a junior high school working with the College, encouraging the use of technology in the classroom. It was there I was approached by a professor from the school of Education at UHV who, after finding I was the only one who could answer her questions, asked me for my resume. I've been at UHV ever since and have moved from technology trainer to network specialist, to building a network/server team and last year, turning that team over to my top guy to fill the role of ISO.

**How did you come to the security field?**
"Other Duties As Assigned"
Sadly, the higher ups didn't support the presence of an ISO until they realized we had to have one. I stepped up and said, I'll do it. At the time, I was leading a very capable team of network and server admins and adding security to our services was second nature as all of us were already security conscious.

**Tell us how information security has changed since you started in your role.**
So many ways.
From the technology side, I remember hearing years back that signature based malware detection couldn't last, so it was fascinating to actually watch that process happen, and seeing the results.

From the people side, it's the need to reeducate people on how to keep their information safe. The rise of social media has generated an environment where it's S.O.P. to share everything with the world and it isn't until it's too late when people realize that, maybe, they don't need to share that much. Very difficult concept to get across to college students.

**Who are your users/customers, and what is one of the most challenging areas for you?**
Faculty, staff and students.
Staff are the easiest. They understand their responsibilities, and when shown how to use the tools, they generally use them correctly. The biggest issue is keeping them aware.

Students are next. I've already mentioned the tendency to overshare. There also seems to be a lack of understanding of the responsibility for what happens under their name. Most learn it through some close calls, but some don't learn it until they've experienced first had when someone else is using their Facebook account.

Faculty are sadly the most challenging. While most are great to work with, there are those who make life very difficult because they believe that if they need something to teach or do research, it doesn't matter how they get it. They can be very demanding when if they would just explain their needs, we can almost always meet them in a way which doesn't break any rules.

**How did you first learn about UH-Victoria?**
When the above mentioned professor introduced herself to me. I didn't even know where Victoria was when I met her, didn't know that UH was part of a system. I remember buying a Texas map and searching the index for Victoria and thinking, wow. That's going to be a long drive for an interview.

**What do you like best about your job?**
Two key things. First, the privilege of working with top notch equipment in an environment that promotes learning. Second, the immediate staff around me and especially the student workers I've had while being here. Using one of them as an example, I hired a young lady in 2000-2001. Hard worker, loved to learn, no fear in trying new things. She left to work for Dell and over the next ten years added experience at other big places including RackSpace. She then stepped out of the work force while building her family. But with her youngest starting school she decided to start working again, right at the time I was advertising for my first employee as ISO. The interview team unanimously agreed she was the best for the job and now I have back an outstanding employee with the same drive as from 15 years ago but with incredible work experience and far advanced skills. Being a part of these student's initial work experience is awesome!

**What would people never guess you do in your role?**
I'm really not sure. Since I'm in IT, they believe we all do everything that IT does, whatever that is. You know, computer stuff…

**What other career would you have liked to pursue?**
I really wanted to be a fighter pilot growing up. Learned in high school that my eyesight was too poor for that to happen.

**Have you ever changed career paths?**
Not really. I started hands-on, moved up the ladder, growing my team. If anything, by moving to a dedicated ISO position, I've narrowed my scope, but I believe that'll just make me better in this one area.

**Tell us about your most proud accomplishment.**
Professional: When the dedicated ISO position opened up, the IT director expected me to apply, my staff expected me to apply, everyone assumed I would get the job. It was then I realized I'd be leaving the team I'd formed and led for over a decade. I led the move from a pitiful, 10Mbps thin wire network into the current Gig E to the desktop and 10G between buildings and vital resources. When we started, we had to two Vax's and an Alpha server. Now we have a highly virtualized environment supporting 70 servers hosting databases, email, private cloud file storage and just about everything else a university needs to operate. I didn't want to leave it. But I gave a real hard look at the team and at what had been accomplished and realized I was happy with what I saw and more important, I had a team that could go on without me with the potential to grow far beyond even what I'd envisioned for us. Almost two years later I still feel it when that team faces a crises or gets blamed for something. But I know their skills because I hired them. I know the environment because I designed it. And while I don't know where it's going, I know that team is going to take it far and I'm cheering them on the whole way.

Personal: I've volunteered with the children's ministry for many years at my church. It's something I enjoy and have always been amazed at the potential I see in the kids. But kids grow up. And one who I'd first met when he was 9 or 10, kept in touch with into high school and as he entered the Navy, honored me beyond belief this past summer by having me as his best man in his wedding.

**Top 3 life highlights?**
1. Arriving at Texas A&M as a brand new freshman
2. First time I stood up alone in my church in front of more than 50 elementary school kids. There's the responsibility all those parents were putting on me, there's the need to teach religious concepts at a kid friendly level, and there's the fact these are kids and you never know what will happen. I went on to keep doing it on and off from 1999 until early this year.
3. Twenty years ago last August, getting married to my wife Jane.

**What are your hobbies?**
Photography
Model rockets
Writing

**People would be surprised to know that you….**
Volunteered with the children's ministry at my church for over 10 years and still play Pokémon because of it.

**Any favorite line from a movie?**
Depends on the day…

When I'm feeling cranky,
> Hermione from Harry Potter and the Sorcerer's stone: "What an idiot!"

Before I present to cabinet or other important people, I say this as a reminder to myself to avoid the tech speech:

Korben Dallas from the Fifth Element: "I only speak two languages, English and bad English."

**Are you messy or organized?**
I like to think of myself as functionally messy.

**Favorite travel spot?**
Hawaii, the Big Island.

**What was the last book you read?**
Just finished rereading an old classic, The Complete Works of Sherlock Holmes. Before that I read for the first time The Rise and Fall of the Third Reich by William L Shirer. A fascinating and scary look into that portion of our history.

**What radio station do you listen to?**
My current playlist has Pink Floyd, Evanescence, Newsboys, Swedish Revolution, Finger Eleven and Lindsey Stirling. If listening to the radio in Victoria, I switch between San Antonio's WOAI for news or local classic rock on 106.9.

**If you could interview one person (dead or alive) who would it be?**
Thomas Mims (possible different spelling of last name) my ancestor who came over on the Mayflower.

**If you had to eat one meal, every day for the rest of your life, what would it be?**
Double Dave's buffet.

**Least favorite food?**
Lima beans. Most disgusting thing disguised as a vegetable on the planet.

**If you were to write a book about yourself, what would you name it?**
"Wait, Why Did You Do That Again?"

**Describe what you were like at age 10.**
At 10 I was the perfect child, loved by everyone, adored by my parents. Strangely, many referred to me as an obnoxious punk but clearly they didn't know what they were talking about.

**What is your hidden talent?**
Ha! It's hidden. Maybe in a few years.

**What is the best advice you have received and that you have used?**
"Get off your rear-end!" – My dad

**What would be your advice for a new security professional?**
1. Be honest. It's a lost art in some areas with people not wanting to hurt other's feelings. But sometimes you have to, in a professional manor, tell people the facts and what needs to be done. They may not like it, but if they're professional too, they'll listen and the right things will get done.
2. Learn to identify right from wrong regardless of perceptions and always stick with what's right. In higher ed, too much focus is on perceptions and feelings while facts and logic are deemed insensitive and in some cases unnecessary. But when a professor brakes the rules and now we're looking at a possible FERPA violation with an entire class of students, there isn't time to ease hurt feelings. What's right? Everything else can wait.
3. Learn the art of professional persuasion. And in conjunction, know your environment so well you can demonstrate exactly why security is so important to each individual.
4. Learn your strengths and use them, focus on them, making them even stronger. Building on that (tongue in cheek) learn your weaknesses and hire someone to cover for them.

University of Houston-Victoria may be the smallest member of the UH System but we've got incredible potential and have demonstrated awesome growth, even recognized as the seventh fastest growing university in the past decade. We pull in an incredible mix of traditional and nontraditional students and because of this, have a very high percentage of off-site and remote students which lead to our schools creating outstanding online programs.

# OCISO Corner – Getting to Know the Team

Jeffrey Rogers, CISSP
DCS Security Program Manager
Department of Information Recourses

**What is your responsibility in DIR and with the State?**

I have a very challenging role of managing the security for Texas' consolidated data center and the services offered in Texas DIR's Data Center Services contracts. This is a dynamic and extensive environment where I apply myself towards managing the risk of the systems and their data.

**When and where did you start your career?**

I suppose that this would have to include pieces that might not be cybersecurity, but all added together led me to where I am now. It all began when I graduated from Texas A&M in 1993 and went into military intelligence for the next 5 years. Once I left the military, I started working corporate IT. As I changed roles and organizations, the career in IT and Cybersecurity management materialized.

**Why security field?**

The security field in IT was developing in parallel with my career in IT. It had a great draw to me and was a logical match to my military background. It combines a lot of the things that I am interested in and had what was shaping up to be a great future.

**What is your personal back ground (born/raised/school/family?)**

It is difficult to find a more native Texan than me. My Texas roots go back to the 19th century. My great-great-grandfather was the District 49 Representative for the 18th Texas Legislature. I am a product of the Texas public school system, veteran, and Aggie. While in the military and living in Europe I met my wife. We have three awesome children (two in HS and 1 MS) who amaze me every day.

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

As a child I was hooked from the time I went to see Star Wars in a drive in theater. While I knew that we wouldn't ever get to those levels within my lifetime, an astronaut would be the closest that I could get. As I grew older and I was dead set on being an FBI Special Agent. This led me to studying international politics, joining the military, and learning Spanish and Arabic. I pursued this dream all the way up to one test to go between me and Quantico, but decided to withdraw myself from the process and continue with my IT career.

**What is the greatest lesson you have learned?**

It is important to always be open, honest, fair, and do your best; the rest will fall in the right place. I have learned not to worry about things that are outside of my sphere of influence – better to use those energies to improve the things in your sphere.

**What do you want your legacy to be?**

I don't have enough wisdom to be able to answer this question yet.

**Do you have a favorite hobby or pastime?**

While in the military I developed a love of running and have completed half-marathons and triathlons. I have always loved to play basketball. Some injuries combined with the years have really curtailed those activities in the last few years. I still love the outdoors and fishing. It has been many years since I hunted but that is also enjoyable. Right now I am perfectly content to just spend as much free time as I can with my family.

**What do you like best about working at DIR?**

My favorite thing about working for DIR is the mission. I really believe in what they are trying to do for the State and think it is where we need to go.

# Insight from our Texas CISO

## Community

*Eddie Block*
*CISO, State of Texas*

Texas state government is a collection of over 150 distinct and individual state agencies and institutions of higher education. As a native Texan, I appreciate the individualistic nature of our citizens and our state government.

In order to protect those citizens, though, we must work together as a community of information security professionals to share successes and failures, develop a strong infrastructures, and prepare for whatever risks the next generation of technology throws our way.

One of the things I think DIR has done well over the past few years is to build a stronger community through multiple working groups and events. Whether the Statewide Information Security Advisory Committee (SISAC), Information Security Officer Working Group (ISWG), the Information Security Forum, webinars, discussions, or meetings, we interacted with security professionals at 87% of the state's agencies and institutions of higher education in the past year.

Through these collaboration opportunities, you have been able to share your ideas, concerns, and challenges with the OCISO. It is exciting to see and hear of collaboration efforts amongst different entities, whether or not DIR is involved.

I'm also working to build community amongst the states. In October, I attended the National Association of State Chief Information Officers (NASCIO) annual meeting. Discussing challenges and successes with other state CISOs in attendance I saw some places where Texas is ahead of the curve, but also areas where we can make some improvements.

As I write this note I'm heading to the MS-ISAC annual meeting. In attendance will be security professionals and fusion center representatives from states, cities, counties and other public sector entities. We will discuss ways that we can all work together better and how we can leverage federal resources to bear on the threats we collectively face.

I believe that discussion of these challenges helps everyone at the table evaluate their own risk, their own security program, and generates ideas that we can all use. So this month, I urge each of you to reach out to a colleague at another agency and grab lunch together. Discuss your challenges and solutions and help us build a stronger Texas security community.

*Eddie Block*
*CISO, State of Texas*

# Events

## 2015 Save the Dates

- Austin ISSA Brings Chris Hadnagy to Austin, December 10 – 11
- TASSCC State of the State Conference, December 11

## Austin ISSA Brings Chris Hadnagy to Austin

December 10–11, 2015

Austin, Texas

Austin ISSA is bringing best-selling author and expert social engineer **Chris Hadnagy** to Austin for two days in December!

Chris will teach **Advanced Open-Source Intelligence (OSINT) for Social Engineers** on December 10 and 11, 2015. This training is valuable for security incident responders, security analysts, forensic analysts, security architects, red team members, blue team members – anyone who needs to understand how social engineers con employees into enabling break-ins.

This class is normally $1800, and Austin ISSA is able to offer reduced pricing for this one-time event:

- General admission for ISSA members: $1199
- General admission for non-members: $1299

Don't miss this opportunity to learn from the guy who literally wrote the book on social engineering!

To read more and register visit https://austin-osint-2015.eventbrite.com

For the fastest response to questions, send email to education@austinissa.org

# OCISO Participation Around the State

- MSISAC Annual meeting held November 16-18 in San Diego, California. Eddie Block and Suzi Hilliard attended.
- MPA University of Texas Cyber Fraud Presentation held December 3. Claudia Escobar will be judging the presentation.
- State of Arizona Supervisory Control and Data Acquisition (SCADA) Cybersecurity Tabletop Exercise (TTX) held December 8. Eddie Block and Claudia Escobar will be attending.
- Virginia Information Technologies Agency (VITA) representatives will be at DIR December 7-9. Claudia Escobar will be attending.

Feedback, comments, stories, etc.
DIRSecurity@dir.texas.gov