



DIR Cybersecurity Insight Newsletter

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

Stop



Stop: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

Think



Think: Take a moment to be certain the path ahead is clear. Consider how your actions online could impact your safety or your family's.

Connect



Connect: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

About Stop -> Think -> Connect.

STOP. THINK. CONNECT.™ is the first-ever coordinated message to help all digital citizens stay safer and more secure online. The message was created by an unprecedented coalition of private companies, nonprofits, and government organizations.

Our goal is to help Americans understand not only the risks that come with using the Internet but also the importance of practicing safe online behavior.

Contents

Security 101	
Identity Theft	2, 3
Texas Information Security Program Updates	
SANS – Securing the Human	4
InfoSec Academy	4
Our State ISO Spotlight	
Shenny Sheth	5, 6
Collaboration Opportunities	
Policy Subcommittee	7
From our State CISO	
Awareness month	8
Events	9

Security 101 - Identity Theft

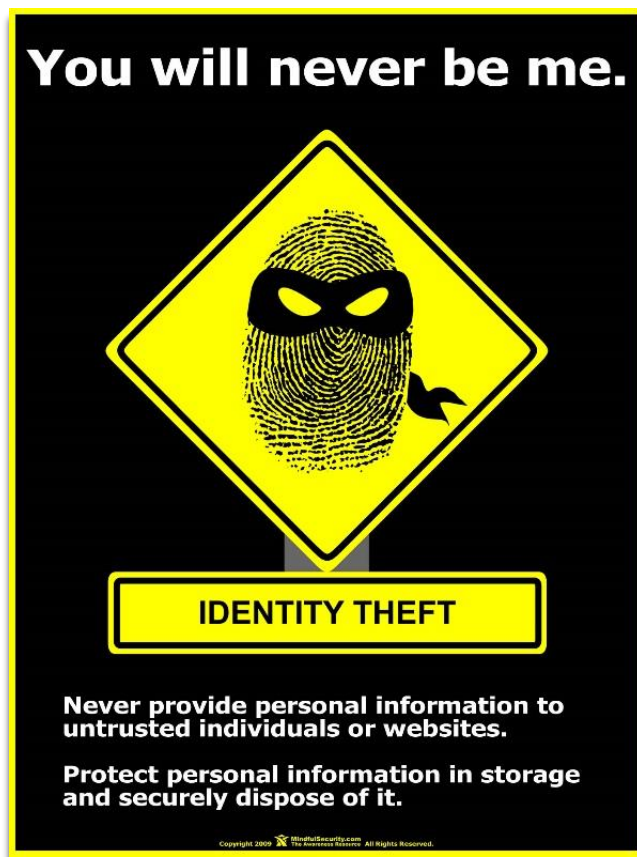
Identity Theft

A growing concern, with all of the Internet access to financial and identity information, is the theft of your good name, who you are, your identity itself. In brief, someone could steal your credit card information and buy things with your money, ruining your credit. They could copy your driver's license or Social Security number and then associate their face with that info. Their next step could be getting bank loans or making large purchases in your name and leaving you in the lurch to clean up the mess they left. While it's impossible to completely protect your identity, there are several steps that can make it more secure, thereby making it harder to go after you than someone else who may be a much easier target.

Many banks and institutions that have your personal information have a policy under laws and regulations to either opt-in to allow your info to be shared with other companies or to let you opt-out. This data, including your name, address, age, and other personal details, such as purchasing habits, credit rating, or educational background, are often shared with third party companies for marketing or targeted advertising or can simply be resold to other companies. Make sure you contact any institution or company providing you services (e.g., banks, insurance companies, etc.) and request that it be kept private; the fewer companies that have access to any of your personal information, the better.

Most major accounts, specifically banks, credit card companies and public utilities like telephone or hydro services can assign a password or pin number to the account that you have to verbally relay over the phone before effecting any changes or retrieving any information often. The phone conversation with these firms will begin with the request of that PIN and confirmation of your address before they will answer any questions whatsoever. If you haven't already, proactively call any companies with which you have an account and request a password for your account to help protect you from having unwanted information shared or even having a service like your phone canceled by someone else without your consent.

A paper shredder is a cheap and easy investment – shred anything with an account number or personal info before throwing it away or recycling it. Many banks or institutions will accept an original bill with your name and address as a form of identification for creating a new account, so it can be as valuable to a thief as your driver's license when creating an account in your name. By shredding it, you not only stop them from being able to do this, but you can still recycle the paper to your heart's content.



"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."

What does “to be aware” mean?

Being security aware means you understand that the potential exists for others to deliberately or accidentally steal, damage, or misuse the data stored within a company's computer systems and throughout its organization. You understand the risks, and every decision is made based on that risk appetite.

Are there ways to avoid being a victim?


Unfortunately, there is no way to guarantee that you will not be a victim of online identity theft. However, there are ways to minimize your risk:

1. *Do business with reputable companies* – Before providing any personal or financial information, make sure that you are interacting with a reputable, established company. Some attackers may try to trick you by creating malicious web sites that appear to be legitimate, so you should verify the legitimacy before supplying any information (see [Avoiding Social Engineering and Phishing Attacks](#) and [Understanding Web Site Certificates](#) for more information).
2. *Take advantage of security features* – Passwords and other security features add layers of protection if used appropriately (see [Choosing and Protecting Passwords](#) and [Supplementing Passwords](#) for more information).
3. *Check privacy policies* – Take precautions when providing information, and make sure to check published privacy policies to see how a company will use or distribute your information (see [Protecting Your Privacy](#) and [How Anonymous Are You?](#) for more information). Many companies allow customers to request that their information not be shared with other companies; you should be able to locate the details in your account literature or by contacting the company directly.
4. *Be careful of what information you publicize* – Attackers may be able to piece together information from a variety of sources. Avoid posting personal data in public forums (see [Guidelines for Publishing Information Online for more information](#)).
5. *Use and maintain anti-virus software and a firewall* – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall (see [Understanding Anti-Virus Software](#) and [Understanding Firewalls](#) for more information). Make sure to keep your virus definitions up to date.
6. *Be aware of your account activity* – Pay attention to your statements, and check your credit report yearly. You are entitled to a free copy of your credit report from each of the main credit reporting companies once every 12 months (see [AnnualCreditReport.com](#) for more information).


Source: www.us-cert.gov/ncas/tips/ST05-019

Stop.Think.Connect.™


Tips for keeping your personal information safe, your family protected, and our national security intact.




Stop hackers from accessing your accounts — set secure passwords.
Stop sharing too much information — keep your personal information personal.
Stop — trust your gut. If something doesn't feel right, *stop what you are doing*.



Think about the information you want to share before you share it.
Think how your online actions can affect your offline life.
Think before you act — don't automatically click on links.



Connect over secure networks.
Connect with people you know.
Connect with care and be on the lookout for potential threats.



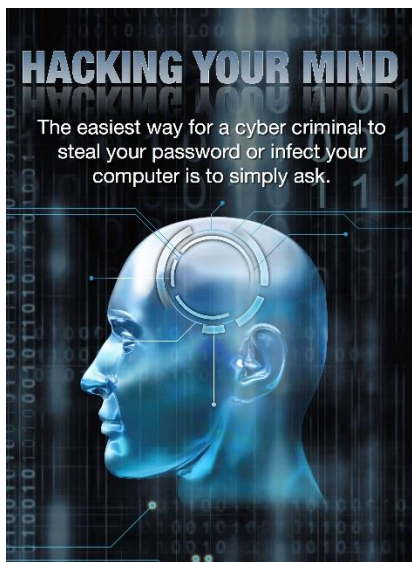
STOP | THINK | CONNECT™

Securing one citizen, one family, one Nation against cyber threats.

www.dhs.gov/stophinkconnect

What does your awareness program look like? It is effective? How do you measure its effectiveness?

Security Program Updates



SANS Securing the Human Training Program Updates

Licenses are still available

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

Do you need metrics?

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

Texas InfoSec Academy Open House

The Office of the Chief Information Security Officer (OCISO) is hosting two open houses for the Texas InfoSec Academy on October 17, 2014, from 10:00 AM until 12:00 PM and on October 21, 2014, from 2:00 PM to 4:00 PM at the William P. Clements Building, 300 W. 15th Street, Austin, Texas. This event, open to Information Resource Managers and Information Security Officers from state agencies and higher education institutions and will provide attendees the opportunity to learn more about the InfoSec Academy curriculum. This curriculum is comprised of courses in four different areas of study including the Texas Security Policy and Assurance course, security and security certification review courses, and soft skills courses. A roadmap for those pursuing specific security certifications will be provided. Attendees will also get a chance to preview the new InfoSec Academy Learning Management System.



Coffee break and learn



Find out more about the InfoSec Academy curricula, meet the instructors, and get registered!

Details in the "Events" section.

Information Security Officer Spotlight



Shenny Sheth, PMP, CISSP, C|CISO
DADS Information Security Officer

I see that the "hide me, shield me" attitude of yesterday is replaced by today's netizen announcing "find me, follow me."

I grew up in central-western parts of India. My father coached me early on importance of education and cultural diversity while mother shaped a life-long traveler in me. Upon completing an Electrical Engineering degree, I moved to the U.S. for advanced education in technology with a special concentration in the Japanese language. During my college years, I began my career with the Texas Center for Superconductivity at University of Houston.

How did you come to the security field?

I also worked in private sector. I discovered quickly that barriers existed that often made security of enterprises a daunting undertaking, requiring tenacity and perseverance. In the modern world, everything an organization does with its innovation, data, technology, processes, and services immediately becomes part of its information architecture, which requires continuous protection regardless of the entity's mission. Quite frankly, I got drawn to solving this challenge of security, disaster recovery, and IT service continuity. So, management of it has become my passion for the past six years at the Texas Department of Aging and Disability services (DADS)!

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

I see that the "hide me, shield me" attitude of yesterday is replaced by today's netizen announcing "find me, follow me."

My key observation is that higher speed networks are emerging and always-on computing power has converged in the hands of data-hungry users. All it takes is a single weakness. For example, one missed opportunity to marshal personnel to harden a system could let in a relatively low

effort exploit, ultimately causing immense harm to the organization.

Information security was once considered as a behind-the-scenes network access control function. It is now being delivered in the form of informed risk management activity, whether the process is system development life cycle or IT change management flow.

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

Nearly 18,000 multidisciplinary staff directly or indirectly use automation relying on some form of information security assurance services at the agency. Offering the workforce encrypted computing devices, software applications with baked-in safeguards, and networks able to repel cyber threats without failure are my biggest daily challenges.

Tell us about your most proud accomplishment.

The most memorable and proud moment for me was during FY13 when an independent assessment of the DADS agency's security program revealed the highest overall maturity status amongst comparable entities reviewed within Texas. Key to this success were unwavering executive support, ability to achieve exceptional funding, and relentless work of the security, IT, and vendor personnel

Texas Department of Aging and Disability Services | DADS

The DADS mission is to provide a comprehensive array of aging and disability services, supports, and opportunities that are easily accessed in local communities.

Do you have family in Austin?

Yes, call us Austinites, yet we are a highly intercontinental family! My wife Yoshie, originally from Tokyo, and I are married for nearly 20 years now. Our two sons, born here in the U.S., are students of the Liberal Arts and Science Academy High School in Austin. Our busy life revolves around them.

What are your hobbies?

I love people, architectures and landscapes. Things I do most when free are reading, watching movies, traveling and experimenting with photography.

People would be surprised to know that you...

Aha, knew you would ask! When I came to Austin in 1998, there was an intrinsic desire to learn more about the city and its people. So I immediately joined the Austin Citizen Police Academy. I served as the 39th President of the Academy, rode nightly with the officers in interesting parts of the City and visited every division of the Police Department, including their High Tech Crime Unit.



Shenny with the Assistant APD Chief 1999

Any favorite line from a movie?

From a 1982 movie GANDHI: "Where there is injustice, I always believed in fighting. The question is: do you fight to change things or do you fight to punish?"

Are you messy or organized?

Family thinks that I am a minimalist, therefore organized.

Favorite travel spot?

Nikko National Forest located in Tochigi Prefecture of Japan, which is on UNESCO's World Heritage List. It's just magnificent!

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

It would be some form of a memoir. I do not yet have a catchy title to dispense.

What advice would you give to a new security professional?

Know your organization's mission, lines of business, and methods used for business service delivery. Wrap security around these aspects by dedicating funding and personnel, instituting select program components, and maintaining ongoing governance of all. Seek an independent assessment or internal audit of your program. Progressively implement program changes, formally report to the agency head or designated representative annually, train staff and yourself, and continuously measure effectiveness.

Collaboration Opportunities

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

Policy Subcommittee

- **Goals**
The Policy Subcommittee is charged with advising DIR on information security polices, rules, and guidelines.
- **Structure**
Edward Block, Deputy CISO, chairs the group and provides much of the “straw man” policies for the group to review. Eddie also serves as the subcommittees interface into the SISAC.
- **Members**
The subcommittee currently has 22 members, representing all articles of government (except the legislative), several of our state’s institutions of higher education systems, and the private sector.
- **What are we working on?**
Finishing a revision to TAC 202 and developing the new control catalog. The TAC 202 update and control catalog will be published for public notice and comment in November 2014.
- **What are the plans?**
The subcommittee will continue to review the TAC 202 control catalog on a biennial basis. Additionally, the subcommittee will address other policy issues, as requested by the SISAC.
- **What we have achieved**
In January, DIR published the Agency Security Plan template for agencies to use when reporting their security plans as required by 83(R) SB1597. The Policy Subcommittee was integral in responding to the legislation quickly.

Edward Block
Deputy Chief Information Security Officer
Department of Information Resources
State of Texas

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

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

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

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

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

Solutions Subcommittee
Claudia.Escobar@dir.texas.gov
Statewide Security Program Manager, Department of Information Resources

Join a Team

Insight from our Texas CISO

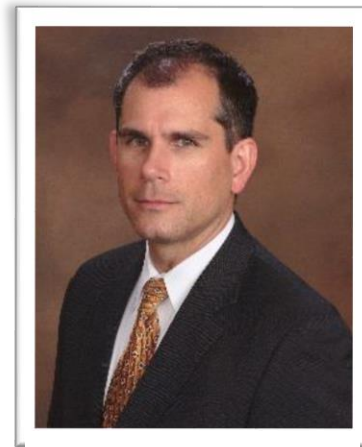
As you read this article, October as National Cybersecurity Awareness Month and Texas Cybersecurity Awareness Month is in full swing. For a full 31 days during the month, you should see a flurry of awareness campaign notifications and messages providing tips and information to help encourage a safer online experience. That is perhaps the most important distinction to the awareness month activities over the type of information that seems to flow the other eleven months of the year, and something that should be considered as the primary objective of creating awareness: providing actions that help improve cybersecurity.

Amidst the constant stream of security incident announcements and information security breaches, I find myself picturing Marcus Aurelius, played by Russell Crowe in "Gladiator," standing in the middle of the Coliseum in Rome shouting "Are you not aware? Are you not aware?" But the awareness generated by these events is not accompanied by the necessary action needed for individuals or organizations, only what we might hope would be motivation to improve. Too often we do not look deep enough into the underlying factors that lead to these events to identify causes or the activities that will generate improvement when the event does not impact us directly. Instead we may breathe a sigh of relief and go about our routines. Consider also that the heightened state of awareness can also be overwhelming, creating a paralysis and helplessness, especially when the events seem a world away.

Connecting awareness with personal impact can help to ensure a positive response, but without clear direction on actions, awareness can quickly be lost among other priorities. Awareness must also inspire a desire for change, whether in an increased desire for understanding and learning or actual changes in behaviors and improved cybersecurity. Awareness by itself is not enough, and it will certainly not be sustained if only approached for one month of the year.

Once October concludes, spend some time thinking about how to carry forth the initiatives of Cybersecurity Awareness Month throughout the rest of the year, and evaluate the ways that you can connect awareness with specific actions that must be performed to achieve your results. Focus on distinct steps and actionable plans. Put it all together with some measureable outcomes and success criteria related to specific risks that your organization faces, and see if you can't start on a Cybersecurity Awareness Year. Kind of sounds like an information security program, doesn't it?

Brian Engle
CISO, State of Texas



Brian Engle

National Cyber Security Awareness Month Events

Get Involved!

National Cyber Security Alliance

Week 1 Twitter Chat: STOP. THINK. CONNECT. : Online Safety for Everyone

Week 2 Twitter Chat: How to Build a Safer, More Secure and Trusted Internet

Week 3 Twitter Chat: Securing the Internet of Things

Week 4 Twitter Chat: Keeping Your Business Safe Online



See more at: www.staysafeonline.org/ncsam/events

Use #ChatSTC to join

Department of Homeland Security

Cybersecurity for Small and Medium-Sized Businesses and Entrepreneurs

Capital Factory

Date: Tuesday, October 21, 2014

Time: 12:00 pm - 1:30 pm (CDT)

www.dhs.gov/national-cyber-security-awareness-month-2014

www.staysafeonline.org/ncsam/events

DIR participation in Cybersecurity Events

October 1, 2014, Austin, TX – In recognition of Governor Rick Perry proclaiming October 2014 to be Texas Cyber Security Awareness Month, the Texas Department of Information Resources (DIR) will be participating in the following events:

- Brian Engle, State Chief Information Safety Officer (CISO), presented the keynote address at the joint **Austin and San Antonio Infragard Conference**.
- Edward Block, State Deputy CISO will be presenting at the **City of Hurst TX Regional Cybersecurity Summit Conference** with the City of Austin Deputy CIO on regional cyber response coordination
Date: Thursday, October 16, 2014
Time: from 9:00 am - 4:15 pm
Location: Hurst Conference Center
www.texaspolicechiefs.org/sites/default/files/2014_9CyberSecurityoct15.pdf
- Brian Engle, State CISO will be providing remarks at the **San Antonio Chamber of Commerce cybersecurity event**.
Date: Thursday, October 16, 2014.
Time: 7:30 am - 1:00 pm
Location: Hilton Palacio del Rio Hotel
200 South Alamo Street, San Antonio, TX 78205
www.sachamber.org/wcevents/eventdetail.aspx?eventid=3280#sthash.CmCSAGgX.dpuf

The Office of the CISO will be supporting agency events during October that include:

- **The Health and Human Services Commission** Security Operation Center Open House. Contact: shirley.erp@hhsc.state.tx.us
- **The Texas Education Agency** Cybersecurity Awareness Fair. Contact: frosty.walker@tea.state.tx.us
- **The Department of Family and Protective Services** is integrating cybersecurity training within their employee training using SANS Securing the Human and launching biweekly discussions of the latest security topics in their DFPS Connect Newsletter. Contact: mark.herber@dfps.state.tx.us
- **The University of Texas - Dallas** has a variety of campaigns launching to create outreach and awareness, including a workshops for securing BYOD and a launch of their first Information Security Office pamphlet that will be distributed throughout the campus. Contact: nxh141030@utdallas.edu
- **The Texas Workforce Commission** is launching a month-long campaign including weekly emails regarding a variety of information security topics, such as *Keeping your kids safe online*, *Destruction / discarding of old computer tech gear*, *Keeping a clean PC*, *Even the smartest people can be fooled*, and others. Contact: kent.dyer@twc.state.tx.us
- **Office of the Attorney General** will be conducting a security awareness survey of its employees, will display Securing the Human posters to enhance visual awareness, and post monthly security-related articles in their internal newsletters. Contact: suzi.hilliard@texasattorneygeneral.gov and arturo.montalvo@texasattorneygeneral.gov

Training and Conferences around the State

InfoSec Academy Open House

Date: Friday October 17, 2014.

Time: 10:00 am - 12:00 pm

Location: 300W 15th St. Clements Building, room #103

Date: Friday October 21st, 2014.

Time: 2:00 pm - 4:00 pm

Location: 300W 15th St. Clements Building, room #103

Monthly Security Program Webinar

Tooling Up for Incident Response

Date: October 14, 2014.

Time: 2:00 pm CDT

Info: <https://www1.gotomeeting.com/register/119146696>

CISSP Training Class

Date: October 20-24, 2014

Location: Stephen F. Austin Building, Austin

Info: Contact Brandon Rogers (Brandon.Rogers@glo.texas.gov)

InnoTech Austin

Date: October 15, 2014

Location: Austin Convention Center

Info: www.innotechconferences.com/austin/

Houston Security Conference (Hou.Sec.Con)

Date: October 16, 2014

Location: Derek Hotel, Houston

Info: houstonseccon.com/v5/

BSides Houston

Date: October 18, 2014

Location: Site TBD, Houston

Info: www.securitybsides.com/w/page/81064187/BSidesHou

See the full list of Texas BSides events at:

bsidestexas.blogspot.com/



Feedback, comments, stories, etc.

DIRSecurity@dir.texas.gov



Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas



STATE OF TEXAS
OFFICE OF THE GOVERNOR

As a state and nation, we are increasingly reliant on the Internet. Individuals, schools, libraries and businesses use the Internet to communicate, manage finances, enhance education and conduct business. This technology has become crucial to our telecommunications, transportation, financial services, retail, health care, emergency response systems and more.

Unfortunately, Internet users and the information infrastructure they use face a growing threat of malicious attacks by viruses and loss of privacy from spyware and adware intrusions. We also must stay vigilant against criminals who would commit identity theft and fraud online.

Each October, an awareness campaign is conducted to promote safe habits among Internet users.

At this time, I encourage all Texans to educate themselves about keeping personal information secure, current online fraud schemes and other basics of cyber security.

Therefore, I, Rick Perry, Governor of Texas, do hereby proclaim October 2014 to be

Cyber Security Awareness Month



in Texas, and urge the appropriate recognition whereof.

In official recognition whereof,
I hereby affix my signature this the
18th day of August, 2014.

Rick Perry
Governor of Texas