

THE DIR CYBERSECURITY INSIGHT

★ ★ ★ ★ ★ ★ ★ July FY2016 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV ★ ★ ★ ★ ★ ★ ★

Land of the Free Wi-Fi

A latte, scone and free Wi-Fi may be the essentials at your favorite afternoon hangout, but the “free” Wi-Fi may come at higher, unexpected cost. It's worth doing your homework before selecting any open or unfamiliar networks to figure out what your device is automatically connecting to.

Once you connect to a hotspot, most devices default to automatically remember and connect once you're in range again. So as soon as you get home, or return to your regular coffee shop, your device is online again! How convenient! And how risky...

Smart devices and laptop frequently send requests to identify “known/trusted networks”. This means you have a continually expanding list of trusted networks.

You can check to see how many saved Wi-Fi networks you have.

Open your control Panel -> Network and Internet -> Manage wireless connections

How many are set to “*automatically connect*”? How many of these are public networks?

Hackers can all too easily utilize this setting to steal your data with a man-in-the-middle (MITM) attack. A “free Wi-Fi” or “known network” variation is set up leading users to believe the source is trustworthy and legitimate.

Protect yourself from the man-in-the-middle:

- Make sure you are connecting to the correct SSID
- Use HTTPS in your websites
- Use VPN when available
- Never use the same passwords on social networks and other accounts (banking, credit card sites, etc.)
- Avoid financial transactions over a public connection

CONTENTS

Monthly Article

Land of the Free Wi-Fi P.1

Program Updates

InfoSec Academy P.2

SPECTRIM P.2-3

CPT P. 4

Our State ISO

Spotlight

Danny Miller P.5

Security Corner

Jeremy Wilson P.6

From our State CISO

p.7

Events

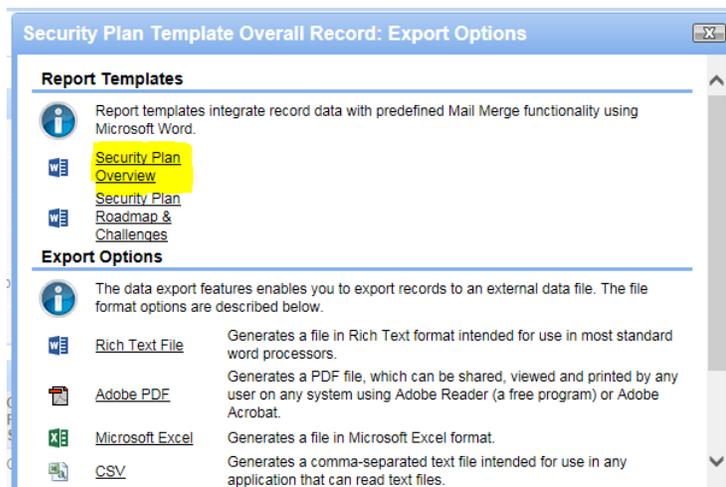
p.8

InfoSec Academy Update

The InfoSec Academy is now live! DIR is proud to be partnering with New Horizons for this endeavor. The Academy offers several libraries of courses and resources for On Line Anytime learning (OLA) along with On Line Live (OLL) certification preparation courses. The Texas Security Policy and Assurance course is required before taking any of the OLL certification preparation courses. This course offers both a computer-based OLA course, and as an Instructor-Led Training (ILT) course. The next live ILT will be Friday, August 12, from 8:00 – 4:00, at the New Horizons Austin location: 300 E Highland Mall Blvd, Suite 100 - Austin, TX 78752. If you would like to sign up, [VISIT THE INFOSEC ACADEMY](#) website. The OLA version of the Texas Security Policy and Assurance course will be available soon! If you have any questions about the InfoSec Academy, [visit our website](#) or send an email to infosecacademy@dir.texas.gov.

SPECTRIM

There is now a report available in SPECTRIM where you can make a Word document of your security plan template (SPT) and distribute to your agency leadership. In order to create this file, you need to perform the following steps:

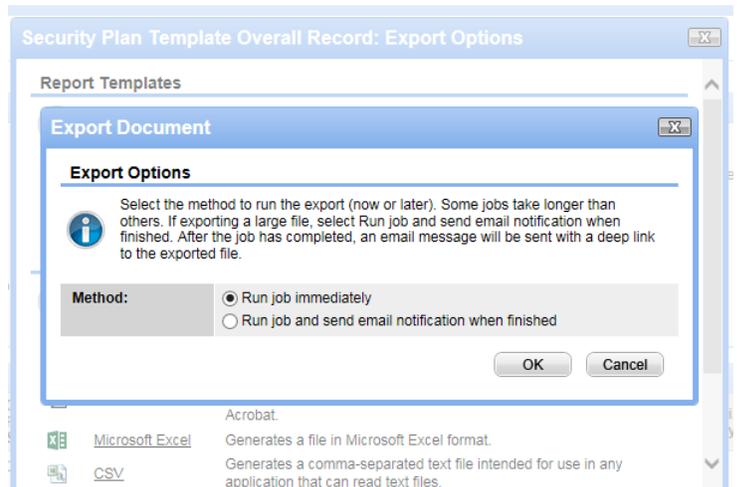


Pull up your overall SPT record in SPECTRIM. Click on the Export icon in the upper right hand corner as shown to the left. You will see two options: SPT overview or SPT Roadmap and Challenges. Click on the option you prefer.

You will be able to choose to run the export real time or batch in the background. This is a standard Archer option. However, this report is small so you should be able to run it in real time without causing a disruption to your work. Choose your option and click OK.

Once the export is complete, you can then download the file.

Below are examples of the two options created with this process.





SECURITY PLAN CONTROL STATUS

Organization Name: State Agency for Archer
 Overall Status: In Process with Management

Submitter: Sally, Smith
 2016

Objective	Functional Area	Maturity Level	L0 %	L1 %	L2 %	L3 %	L4 %	L5 %
Privacy and Confidentiality	Identify	4	0	0	0	0	50	50
Data Classification	Identify	1	0	100	0	0	0	0
Critical Information Asset Inventory	Identify	2	10	0	50	50	0	0
Enterprise Security Policy, Standards and Guidelines	Identify	1	0	90	10	0	0	0

REMINDER: Enter your cybersecurity funding requests into the Cybersecurity/Legacy Modernization application in SPECTRIM. Last session's appropriation bill, HB 1 Article IX, Section 10 requires DIR to submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the October 2014 Legacy Systems Study to be considered for funding to the Legislative Budget Board by **October 1, 2016**. In order to be included in this prioritization, agencies must submit information about their requests to the department through the SPECTRIM online application. [Find additional information](#) including a webinar recording that presented this function.



SECURITY PLAN CONTROL ROADMAP AND CHALLENGES

Organization Name: State Agency for Archer
 Overall Status: In Process with Management

Submitter: Sally, Smith
 2016

Maturity Levels

Level	Level	Description
5	Optimized	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.
4	Managed	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
3	Defined	The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.
2	Repeatable	The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
1	Initial	The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
0	Non-Existent	There is no evidence of the organization meeting the objective.

Objective	Maturity Levels	Controls Needed	Challenges to Implementation
Privacy and Confidentiality	4	This organization needs to immediately complete the	<ul style="list-style-type: none"> Inadequate Funding Lack of Planning to Develop Roadmap No Changes Needed

Controlled Penetration Tests

Ransomware is malicious software that, once successfully installed, disables a user's PC or ability to access critical work (usually by encrypting files) until users pay to have access restored. It typically disguises itself as helpful software, like antivirus or anti-malware programs, in order to get users to install it. Preferred methods recently have even included phishing attacks via emailed URL links and social engineering – attackers calling targets and claiming to be members of law enforcement.

Once prevalent in Russia and Eastern Europe, ransomware has spread to the US and has become a source of frustration for private users and concern for organizations. According to a recent industry-perspective opinion poll on GovTech, ransomware is listed as one of the top 10 cybersecurity issues we'll face in 2016.

In February 2016, Hollywood Presbyterian Medical Center in Los Angeles, CA, paid approximately \$17,000 to ransomware attackers to gain access to their electronic records systems, including crucial patient information. Kansas Heart Hospital in Wichita, KS, twice became victims of ransomware in May 2016. Besides the illegality of extortion, impeding a healthcare facility can also endanger lives.

There are precautionary practices to put in place in case of a ransomware attack. Have a good backup policy in place and ready for implementation. Even when ransoms are paid, there is no guarantee that a malicious attacker will honor their end of the deal. Restoring from a backup can get your system(s) back on their feet using a previous version of itself. It may be a headache to lose days- or weeks-worth of work, but it beats the alternative. Use a layered defense approach. Don't just have antivirus monitoring your system. Have a good firewall, web-filter, IPS/IDS and/or anti-malware software installed as well. Keep your system OS, web plug-ins and security software up-to-date with the most recent definitions and patches. Most ransomware attackers are opportunistic and target known vulnerabilities, rather than utilizing a zero-day attack. Routinely check user privileges. If a basic user has elevated privileges and finds themselves compromised via ransomware, the attacker will usually assume the same rights as the user they infect. This can create havoc for network and shared drives. Educate your users. Ransomware attackers are utilizing phishing and social engineering to get users to install their software. Their intent is to exploit a person's natural tendency to cooperate and assist. Teach your users to be leery of any suspicious warnings and make sure they're well-informed of their local IT's contact information. It's best that IT be called in to recognize a false positive than a true one.

If you're interested in learning more, please visit Norton's ransomware article database, Ars Technica's Security section, GovTech.com or Computer Weekly's article, "How to avoid being caught out by ransomware."

Information Security Officer Spotlight



Danny Miller
System Chief Information Security Officer
The Texas A&M University System

I've held a variety of positions from software developer to project manager. I was fortunate enough to travel overseas and work as the CIO of a group of E.U.-based companies. After 9/11, I returned to the states to become Dell Computers Global IT Audit Manager. I had a desire to do something entrepreneurial. I took a partnership in a small consulting firm based on the east coast. We later sold the firm to Grant Thornton, LLP. I was able to meet the soon to be System CIO of the Texas A&M System and learned we had many of the same views of IT and cybersecurity. I've been with TAMUS only a couple of years, but have enjoyed my time so far.

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

In the last 10 years information has become more and more valuable, both as a commodity and as leverage. The need for true security professionals is at a peak and there aren't enough to go around. That, and with the proliferation of information, the need to be able to categorize and secure information assets based on their classification has become very important. Security incidents have gone beyond simple hacks and malware and has now taken on many new facets, such as social, political and religious activism, state-sponsored espionage and even state-sponsored cyber-attacks. Those attack vectors have dramatically changed with the actors.

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

It is quite challenging to coordinate policy and direction to all members, who have either an ISO or a CISO. The challenge there is to help facilitate the strategy we've set as an entire membership so that each member can achieve those security goals and objectives within the strategy.

What do you like best of your job?

I like the idea that I am at the macro level, setting strategy, policy and goals for the entirety of the System

membership. I also like very much the colleagues I've met and work with at each of the members. Everyone at each of the members is very willing to pitch in and work with me and the other ISO/CISO's at the other members, which makes the working relationship very satisfying.

Top 3 life highlights

Accepting Christ

Marriage to Jayne, my wife of 25 years

Helping raise two good children

What other career would you have liked to pursue?

My family owns nearly 100 acres in East Texas and I am currently pursuing (as time allows) to get the farm back up and going. I am doing blueberries and pears on the farm. Since it's in the Great Piney Woods area of Texas, there's lots of acidic sandy loam soil. Blueberries love that type of soil and we're busily creating a second and parallel career for me and the family.

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

Winston Churchill. In my reading of some of his writings, he was much more discerning than most people think. I wonder what his take on today's world would be.

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

You don't have to be the smartest. You need to be there persistently pushing forward.

What would be your advice for a new security professional?

There's so much to learn, but remember that your profession is always changing. Stay humble and focused on being the best you can.

Security Corner – Getting to Know the Team



Jeremy Wilson
Security Manager
Department of Information Resource

What is your responsibility in DIR and with the State?

I work at the Network Security Operations Center (NSOC) as the Security Manager. The NSOC provides network and security services to more than 150 customers, primarily consisting of State agencies. With more than 2.8 million public facing IP's and 20+ Terabytes of data traversing our network every day we get to see and react to many different types of threats. This keeps my job very interesting.

Why the security field?

Security was always interesting to me as I began to learn about IT and telecom. It wasn't however until I was selected for a full time position at Camp Mabry as the Texas Army National Guard Information Assurance Manager that I was able to do security full time. That experience was very beneficial to me as I learned a great deal and attended many training and certification classes that were a requirement for my duty position. It was also my first time having a statewide network and security program to manage so I grew a great deal in that time and found the security field very rewarding.

When and where did you start your career?

I started my career in military telecom, IT and security fields. I was an infantryman in the Army. I was very fortunate to have served with 2nd Ranger Battalion 75th Ranger Regiment. When I completed my initial enlistment and was transitioning to the Officer Corps, one of our instructors sold me on the Signal Corps. Signal Corps is a much more technical field than infantry and I knew would provide me with training and experience in the IT field.

What is your personal back ground?

I was born in Heidelberg Germany on an Army base, moved back to the U.S. when I was two and moved around a bit before landing in Dallas. I grew up in Dallas and came to Austin for college. I transferred to Texas Tech, then UT

Austin and graduated from Texas State. That was after I completed my initial enlistment in the Army where I was stationed at Ft. Lewis, which is in the Seattle and Tacoma area. I am continually surprised by how many Texans have never been to the Pacific Northwest. It is beautiful. Go if you get the chance.

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

When we were in kindergarten and asked what we wanted to be, no kidding, I said a pterodactyl. I'm still hoping someday to make that happen. After getting all my hopes and dreams dashed at the ripe old age of five, I settled on many exciting choices through the years: helicopter pilot, firefighter, secret agent, SWAT team etc. I think I always wanted to do something worthwhile and exciting that served a greater good. I believe that in serving my country and state I have been able to achieve those goals.

What is the greatest lesson you have learned?

Even though the IT field is about tools, technology, and metrics it is the people that make an organization successful. In leadership training, I learned that you must be willing to adapt to different situations and personalities. It is important for leaders to communicate effectively and understand that everyone has value on the team. If you invest in people, you will be rewarded in ways you can't always foresee.

Do you have a favorite hobby or pastime?

Sports: tennis, volleyball, soccer, basketball and when I can't play them I like to watch them. If not sports, then I'm really into music and seeing live music.

What do you like best about working at DIR?

I get to serve my state and I really believe in the mission and philosophy. The best thing is the people. It is great coming to work in a place with dedicated, experienced and capable individuals. That is what makes DIR a great place to be.

Insight from our Texas CISO



Eddie Block
CISO, State of Texas

As American as baseball, hotdogs, Mom and apple pie...

As we get ready for the fourth of July, fireworks, a celebration of freedom, and hot dogs, I think about the phrase "Motherhood and Apple Pie." These are meant to be things that no one can argue against, they are universally accepted as good. No one would disparage motherhood and who doesn't like apple pie? Well, honestly, I've never been a fan of apple pie, but you get my point...

So what kind of things should be axiomatic in security? Is it always true that security through obscurity is wrong?

Was Gene Spafford right when he said, "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."¹

I think security is much more complex and nuanced than a pithy statement or soundbite. If security through obscurity was always wrong, then we wouldn't try to keep our data centers anonymous, the President's travel plans would be public record, and I would know how Franklin's makes such good BBQ!

That's not to say that obscuring things is the final solution, but it can be one layer in a defense-in-depth approach. Even Spafford's quote addresses a defense-in-depth approach, though one we can't really put in to action. True security must be layered. I'm not sure many people will argue with that statement (though I can hear my inbox filling up already).

Bruce Schneier famously said, "Security is a process, not a product."² I think that is correct. I once consulted for an organization that told me during the initial technology interview that they had three firewalls in the data center. I was glad to hear it. A few days later, while inspecting the data center, I saw three unopened Cisco boxes up against the wall. Foolishly I asked what they were. "Oh, those are our firewalls." They were not plugged in, they were not functioning, but they did have "three firewalls in the datacenter."

This is an extreme example, but how many of us have had the time to really tune a security appliance for our environment? Are we really using them to their full potential? Even though many vendors are willing to sell you a device that they claim will solve a problem, the device still needs people and process.

Which brings me to people. I often hear, "people are the weakest link," but they may also be the answer. If we can get our users to act as auxiliary security staff, think of the impact it would have on our organizations. But to be that reservist, users must have training and support. They must see security as part of their job.

The security truism should be "As Secure as the layers, processes, and people."

OK, I'll admit it isn't as catchy as "mom and apple pie." Maybe one of you can come up with something better. If so, email me and we may use it for our Cybersecurity Awareness month campaign.

Eddie Block
CISO, State of Texas

¹ <http://spaf.cerias.purdue.edu/quotes.html>

² <https://www.schneier.com/crypto-gram/archives/2000/0515.html>

Events

2016 Save the Dates

- Monthly Gartner Webinar: "Information-Centric Mobile Security: Your Data Can Move Without Leaking" Tuesday, July 12, 10 AM
- NASCIO State CISO Leadership Summit: July 27-29, Charlotte, NC
- BSides Las Vegas: August 1-3, Las Vegas, NV
- Defcon: August 3-7, Las Vegas NV
- 2016 TASSCC Annual Conference: August 7 - 10, Galveston, TX
- 2016 NSA Information Assurance Symposium (IAS): August 16- 18, Washington, DC
- CyberTexas Summit: August 23 - 24, San Antonio, TX
- Innotech Austin: November 17, Austin, TX



THE DIR CYBERSECURITY INSIGHT



Feedback, comments, stories, etc. | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV
