

THE DIR CYBERSECURITY INSIGHT

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

The Internet of Things

How many devices do you have at home connected to the Internet? Can you count how many?

How many social networks do you read or post updates to?

The Internet of Things (IoT) phenomenon, a network of physical devices, is rapidly growing in number of users and devices. With this increase in number, the security risks also increase.

Everything that has an operating system has a backdoor, making it susceptible to hacking and potentially having the primary function of the device altered. For example, a baby monitor connected to a network can be hacked giving the hacker access to the camera and speakers in the monitor. This is only one example of a high risk incident with serious implications.

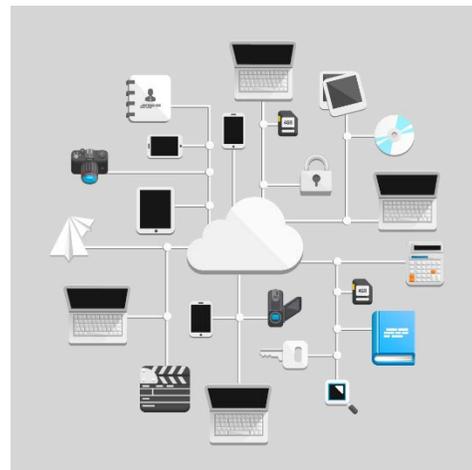
Other examples of devices connected to the internet are vehicles and medical equipment. Google is partnering with well-known automakers to develop an Android platform that will connect their cars to the internet. Locking, unlocking and starting the engine are things that in our mind are already accepted. Now imagine all the internet connected tools and devices that are in an exam or operating room ...scary.

The Internet of Things has great potential for the consumer as well as for enterprises, but not without great risk.

So what can we do?

[FBI Recommends 5 security tips:](#)

1. Understand your IoT devices. Change default passwords and only allow the device to operate on a network with a secured Wi-Fi router.
2. Protect your Wi-Fi networks—set up firewalls and use strong, complex passwords, and consider using media access control address filtering to limit the devices able to access your network.
3. Many routers give you the option to set up more than one network—separate your computing devices from your IoT devices.
4. Disable the Universal Plug and Play protocol (UPnP) on your router.
5. Purchase IoT devices from manufacturers with a track record of providing secure devices and set your devices for automatic updates when available.



CONTENTS

Monthly Article

The Internet of Things P.1

Program Updates

NSOC P.2

Archer P.2

CPT P.2-3

Our State ISO

Spotlight

Mike Day P.4

OCISO Corner

Suzi Hilliard P.5

From our State CISO

p.6

Events

p.7

Network Security Operations Center (NSOC)

Calling all security professionals to the NSOC booth at the Information Security Forum (ISF)! Look for our breakout session on the schedule or stop by our booth for a chat and a grab a bound copy of the 2nd Annual 2015 NSOC Threat Report.

The report this year features a breadth of new data thanks to the implementation of Archer. We have broken this into various subcategories such as data exfiltration, remote access trojans, ransomware and brute force login attempts. NSOC staff will be present at ISF ready to discuss these hot topics as well as other areas of interest.

Aiming to build on last year's momentum, we hope to provide you with a quality report that serves as a useful resource in the future. The goal is to have the report used as a tool not just for security staff, but also for those in leadership roles in state government. We received positive feedback that the 2014 report was useful to help leadership understand security threats from the NSOC perspective.

We look forward to seeing you at ISF. For SSO membership, 2015 NSOC Threat Report questions or any NSOC security questions you may have, I can be reached at Jeremy.wilson@dir.texas.gov.

Archer Updates

ISF is coming! We will have our team at a booth at ISF ready to answer any questions you may have. Drop by and see us at booth #405!

We have recently modified the Risk Application. You can now add divisions to your organizations. This allows divisions to complete their own risk assessments while still giving you visibility. For more information about this see the [risk application updates](#) on the DIR website.

Additionally, we will begin automated notifications in the next few weeks. These notifications are sent to remind risk assessment coordinators that assessments are not complete and to let assessors know they have open findings. If you have some outdated data you would like deleted, please contact us at GRC@dir.texas.gov.

Controlled Penetration Testing Updates

The OCISO would like to focus attention on SQLi, or SQL Injection attacks. They're a common problem seen by our pen testers and we'd like to shed some light on what they are. What is a SQL Injection? It's a code injection technique using SQL to exploit vulnerabilities in a web application's database server. Hackers inject malicious commands into SQL statements and then use those statements to query a web application in order to seize control of it. Once control has been established, hackers can 1) compromise confidentiality by gaining unauthorized access to sensitive information, like user PII, trade secrets, or intellectual property 2) compromise integrity by modifying data through activities like voiding transactions or altering balances or 3) compromise availability by deleting records and collecting it executing a data dump. It is one of the oldest and most prevalent attack techniques used by hackers today.

SQL is simply a structured language for accessing, querying and manipulating data stored on a database management system. So why does this simple language get used in a cyber-attack? It's rather simple, actually. Agencies and businesses alike, use online, database-driven web applications to provide services, sell products, store media, host blogs and provide real-time information. In 2014, the U.S. generated over \$300 billion in ecommerce alone. For an even bigger perspective, check out <http://www.adweek.com/socialtimes/real-time-ecommerce/499958>. With so much information being stored and accessed using web applications, hackers can't afford to ignore it. SQLi becomes a very valuable tool for enticed hackers.

Acunetix.com has a great illustration of a common pseudo-code used by a web server to authenticate.

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement
database.execute(sql)
```

And now, a simple SQLi example is illustrated, below.

```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

So how is using the above SQL statement a problem? If a web application is vulnerable to a SQLi attack, the above statement creates an authentication bypass. What may then happen is a hacker could be granted access to a database using the first account from the query result – likely the administrator's. This is just a simple example. SQLi attacks come in all sizes and complexities.

What can be done to prevent such an attack? MSDN lists three suggested remedies to help protect your web applications from SQLi:

- **Constrain inputs or input validation.** Use input constraints like type, length, format and range of characters for queries that your database will accept. Setup a list of acceptable characters and reject those that are not listed.
- **Use parameters with stored procedures.** Treat input parameters as literal values instead of executable code. This suggestion does not necessarily prevent SQLi, but it can filter parameters commonly-used by hackers.
- **Use parameters with Dynamic SQL.** Web applications using dynamic SQL are more versatile and allows you to build highly flexible applications. It also allows you to build statements that promote more interactivity with users who possess little to no knowledge of SQL. *Though, this can also be problematic since Dynamic SQL requires more use of specialized data instructions and more runtime processing.*

If you would like to learn more about SQL injections, how they work and how they can affect database-driven web applications, contact DIRsecurity@dir.texas.gov.

Information Security Officer Spotlight



Mike Day
Information Security Officer
Texas Lottery Commission

I work for the Texas Lottery Commission where I serve as the agency ISO. I've been with TLC for nearly eight months and enjoy working with a group of very knowledgeable and talented folks. I began my career as a COBOL programmer with Texas Instruments' Data Systems Group. Later, still with Texas Instruments, I was involved with implementing TI DSG's first LANs which at that time, were composed of thick Ethernet, vampire taps, transceivers and repeaters. I then transitioned to the UNIX systems administration arena where I provided services for TI, Texas Comptroller of Public Accounts, Raytheon, and Motorola/Freescale over a span of nearly 20 years. Later, I worked in the Network Operations Center at a local game development company called Trion Worlds. Most recently, before arriving here, I was responsible for Windows desktop support and system administration for Amherst Holdings and its daughter company, Main Street Renewal.

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

Early in my career, prior to the Internet and PCs, information security really wasn't high on the list of serious threats or even a common topic. Since then, information security continues to evolve at an unbelievable pace. Now, practically every business or government organization has staff whose primary, or only, focus is on information security and there's hardly a day that goes by without headlines that report a cyber-security event.

What do you like best of your job?

Learning!

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

Health challenges. I'm a two-time cancer survivor. On my part, remaining optimistic was my best and perhaps my only defense. I credit excellent surgeons, oncologists, other healthcare professionals and the support of family and friends for getting me to a point where I could even be optimistic.

Top 3 life highlights.

Meeting, proposing to and marrying my wife

What are your hobbies?

I like to read and work on projects in and around my house and yard.

Any favorite line from a movie?

"What we've got here is failure to communicate" -- Cool Hand Luke

What books are at your bedside?

The Art of Human Hacking by Chris Hadnagy

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

"I Never Claimed to be Perfect"

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

Never discuss religion or politics at work or parties

What would be your advice for a new security professional?

Never stop learning

OCISO Corner – Getting to Know the Team



Suzi Hilliard
 Statewide Security Program Delivery Lead
 Department of Information Resources

What is your responsibility in DIR and with the State?

I am the Statewide Security Program Delivery Lead for the OCISO. Similar to an account manager, I help information security officers at agencies and higher education improve their security programs. I work with the ISOs and my team to ensure the security services DIR offers are beneficial and valuable.

When and where did you start your career?

I fell into IT by starting off as a software installer and trainer. I have taken several calculated risks along way, which led to contract positions with the state. I eventually landed a full-time job with the Department of State Health Services as a security analyst. Going into the security field has been the best 'accidental' turn my career has taken.

Why the security field?

At first, it was more about finding a job more stable than contract jobs, and there was an opening in security. But the more I learned, the more fascinated I became. It was the path that stuck, and I'm really glad it did. I love all the different facets of security, and the different people I've met by sticking with this field.

What is your personal back ground?

I was born in Minnesota, but we moved to Crosby, Texas when I was an infant. I have a pretty amazing family that includes great parents, two sisters, two brothers-in-law, and a handful of nieces and nephews. I went to school at St. Edward's University in Austin – as soon as I moved here, I knew Austin would be my home.

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

In college, I began working to become a professional mediator. That was until I learned that I would have to go to law school. I had also studied graphic design, marketing and public relations. I knew my career would be more about working with people than a specific trade.

What is the greatest lesson you have learned?

My dad had put me to work in the family restaurant when I was 12. He always told me that no matter how good I am, I'm always replaceable, so I need to do everything in my power to be as close to irreplaceable as I can, then work harder.

What do you want your legacy to be?

Professionally, I want people to know that I have done my best to better protect the data that belongs to the citizens of Texas. Personally I want people to remember that above all, I tried to be kind to everyone and maybe make them smile a little.

Do you have a favorite hobby or pastime?

Photography. I love taking family pictures and capturing those candid moments that happen when you least expect them.

What do you like best about working at DIR?

I like working with people that constantly work harder to improve security for the state. Knowing I'm in a team that's full of incredibly smart and talented people constantly challenges me to do more.

Insight from our Texas CISO

“April Showers Bring May Flowers...”

As a child I was taught the “April showers” song. At the time I didn’t appreciate the rain or the flowers. I didn’t enjoy singing (please don’t ever ask me to join you for karaoke!) and really didn’t understand the message.

Today, I understand the idea of looking through the struggle or gloom to envision the product of effort.

As I look at security programs statewide I see the parallels. Struggling with budget, hiring, technology changes, education and awareness and the myriad other fires we address each day can be gloomy at times, just like a week of rain. These efforts can also lead to successes that bloom year round.

Many agencies are facing the storms as they are building appropriation requests for the 85th Legislative session. I’ve heard a number of people discussing the worrisome prospects for funding with oil prices low causing budget concerns.

DIR was directed in the 84th session to develop a prioritized list of legacy system and cybersecurity projects for the LBB. We have developed a module, leveraging our GRC system to help with this prioritization. Using this module, we can gather the information we at DIR need to help make an informed decision. So while not all projects will receive funding in the upcoming session, I believe that we can communicate the urgency of high priority legacy modernization and cybersecurity projects.

In addition to funding requests, user education and awareness often seems like a thankless job. We, the security community, understand the importance of arming our users and colleagues with the information they need to protect themselves, both at the office and at home. Often we hear complaints of “more training” or “another HR requirement,” but many don’t understand how important it is to be able to recognize a threat before it turns into an incident.

With all of these challenges, though, perseverance will lead to success. By submitting strong appropriation requests for cybersecurity projects, we send the message how important maintaining and improving our capabilities is to our governmental functions. By training our users, we can help open their eyes to the threats they face at home, in the office, and in all aspects of our modern, connected daily life.

Today, living in central Texas in the midst of a lake of bluebonnets, I happily enjoy the beauty that the rain brings. I hope that the “rain” we put into our programs will produce similar blooms of success.



Eddie Block
CISO, State of Texas

Eddie Block
CISO, State of Texas

Events

2016 Save the Dates

- TASSCC Technology Education Conference: April 11
- DIR Monthly Webinar: April 12
- Information Security Forum: April 14-15
- CyberTexas Conference: April 20-21
- Burton research license webinar: more information to come



THE DIR CYBERSECURITY INSIGHT 

Feedback, comments, stories, etc. | [DIR OCISO](#) | DIRSECURITY@DIR.TEXAS.GOV
