

**BEWARE OF  
HACKERS  
AROUND  
EVERY  
CORNER...**



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

DIR  
CYBERSECURITY  
INSIGHT  
NEWSLETTER

## How Scary Is It?

Cyberattacks are increasingly becoming a regular story in the news. Almost every week we learn about new breaches. The topic seems to be so common now that everyone has adopted the motto of "it is not a matter of how but when..." however, let's not fail to act by preventing, because there isn't a plan worse than inaction.

It is scary that there are still some companies that don't do their due diligence. True, compliance isn't security, but we can start with compliance and best practices.

Most breaches in the private and public sector are discovered by a third party, usually by credit card companies investigating fraud, law enforcement investigating other crime, or reported by end users. Only few breaches have been discovered during an effort to update a cybersecurity posture or through self-assessments.

It is frightening to hear these stories, and the cost that is involved when breaches occur. But perhaps the scariest part is their impact. What is truly the risk and impact to these companies/organizations that have experienced these breaches? Have they lost credibility? What are the behaviors of their customers after that incident? Did they really learn from the lessons? What have we learned?

### Contents

#### Monthly Article

How Scary Is It?	1-3
Network Security Operations Center Update	4
Our State ISO Spotlight	
Arturo Montalvo	5-6
Texas Information Security Program Updates	
Archer GRC Portal	7-8
From our State CISO	9
Events	10-11
Austin ISSA Brings Chris Hadnagy to Austin	10
Lonestar Application Security Conference	11

## 5 of the scariest breaches of 2015 (so far)

### 1. CareFirst BlueCross BlueShield

While it may not be the biggest breach of the year by number of records compromised, the CareFirst BlueCross BlueShield breach in May was notable because it highlighted the continued vulnerability of the health care industry. CareFirst discovered the breach as part of a mandated security review that found hackers had gained access to a database that members use to get access to the company's website and services.

In all, 1.1 million members had their names, birth dates, email addresses and subscriber information compromised; however, member password encryption prevented cybercriminals from gaining access to Social Security numbers, medical claims, employment, credit card and financial data.

### 2. Kaspersky Lab

A different kind of cyberattack than the rest on the list, Kaspersky Lab revealed in June that it had discovered an infiltration in several of its internal systems. The attack, which it named Duqu 2.0, was believed to be a nation-state sponsored attack, whose other victims included events and venues with links to world power meetings, including recent negotiations for an Iran nuclear deal. The Moscow-based security vendor said the compromise included information on the company's newest technologies, such as Kaspersky's Secure Operating System, Kaspersky Fraud Prevention, Kaspersky Security Network and Anti-APT solutions and services. The attackers also targeted investigations into advanced targeted attacks, the company said.

### 3. Premera BlueCross BlueShield

In the second of two mega breaches to hit the health care industry so far this year, health insurance company Premera BlueCross BlueShield said in March that it had discovered a breach occurred in January that affected as many as 11.2 million subscribers, as well as some individuals who do business with the company. The breach compromised subscriber data, which includes names, birth dates, Social Security numbers, bank account information, addresses and other information. According to the Seattle Times, the health insurer had been warned last year that its IT systems were vulnerable to a possible attack.

### 4. Hacking Team

The breach of Hacking Team on July 5 led to a cascade of other security threat revelations and had governments around the globe in hot water. The Hacking Team develops spy tools for government agencies, including those that can go around traditional anti-virus solutions. The breach published more than 1 million emails from the Italian surveillance company, revealing its involvement with oppressive governments as well as multiple Flash zero-day vulnerabilities. Since this breach was so recently discovered, more revelations and facts continue to roll out; the full extent of the impact of this breach is still unknown.

### 5. Office of Personnel Management

Revealed in June, the two breaches of the Office of Personnel Management have snowballed into what is arguably one of the biggest cyberattacks in history. The larger of the two breaches, affecting 21.5 million federal workers, was discovered in late May after a separate, unrelated breach hit the agency in April, exposing the personnel data of 4.2 million individuals. While the actors behind the attack haven't officially been announced, reports have tied the attacks to China-based hackers. While details are still emerging about the extent of the attacks and their effect on millions of federal workers, some of the implications have already begun with the resignation of OPM Director Katherine Archuleta.

## Don't be scared, instead be prepared

It seems like security breaches come and go much too often these days, but despite most of these issues being out of your control, you can do simple things to protect yourself.

### Don't overthink, sophistication doesn't guarantee effectiveness

I came across a blogpost from Marcus Carey, CTO and founder of vThreat, in which he does the Stephen Covey for Cybersecurity and lists the "The Ten Principles for Highly Effective Cybersecurity Programs". Personally, I found these pretty straightforward, very much in line with our State environment, and applicable to all agencies regardless of size or budget. So here's an interpretation to each one of these based on the Texas landscape.

#### 1. **DO NOT be overly concerned with another organization's security policy**

Understand your organization, know the rules and regulations for which your information is liable. Although your organization needs to comply with same regulations as some others, it is still unique. Start learning about your organization, its mission and services, and how you can contribute a better and secure way to succeed on those elements.

#### 2. **Limit administrative privileged accounts.**

The quickest way to reduce massive infestations of malware and breaches is to limit administrative accounts throughout your organization. Yes, it can be painful sometimes and maybe would require more help from IT (helping the user to install a printer, etc.) but it also protects your network from malware or backdoors and Trojans.

#### 3. **Patch vulnerable systems and software.**

There are a lot more patches than those automatic patches from Windows. There are also network devices, applications, firewalls that we need to keep updated. This will save you from a lot of headaches in the future.

#### 4. **Do not use unauthorized systems or software.**

When you use illegal software, it is not only ILLEGAL but it is also limited in term of updates. You need to keep your software patched and updated.

#### 5. **Do not use inappropriate content.**

Make it a policy. Let your users know that they should NOT use corporate email accounts for dating and hookup sites. Pornography sites are the quickest way to get compromised on the Internet. The Internet has a memory greater than that of an elephant.

#### 6. **Develop Incident Response and Forensics capabilities.**

When forming incident response teams, it is recommended the team is comprised of all technical disciplines, management, and a public relations/communications lead.

#### 7. **Keep all logs in a forensic-friendly manner.**

Are your logs understandable? How long have you been keeping them? The first time many organizations look at their log management capabilities is after a breach and that's the wrong time to find out it doesn't work.

#### 8. **Know your DNS activity.**

Organizations can't do proper incident response and intrusion scope analysis without understanding what is going on with your DNS.

#### 9. **Continuously test your defense in depth architecture.**

Don't trust in one layer only. And it is not only technology or people, but also processes. Make sure you have a process for each security technology appliance that is in your network.

#### 10. **Be transparent and show people rather than tell them.**

Work in your organization as a team. Work with your systems administrators, network with others to create a secure platform. Work with your business executives and explain the impacts and risk associated on any decision.

*Don't be scared. Be decisive.*

- Claudia V Escobar, CISSP

Deputy Chief Information Security Officer, State of Texas

# Network Security Operations Center (NSOC)

## Verizon's 2015 Data Breach Investigation Report (DBIR) has been released

DIR held a briefing at the Bob Bullock State History Museum to present and discuss the Verizon 2015 Data Breach Investigation (DBIR). As the Verizon DBIR has become a big topic of discussion in the IT Security community, it was beneficial to agencies to have the authors present and answer questions about the report.

### Compromised vulnerabilities:

This article focuses on the section of the DBIR that addressed exploit patching and statistics regarding common vulnerabilities and exposures (CVEs). Verizon's research identified two very interesting facts. First, over 99.9% of the exploited CVEs were over one year old, and the majority were identified in 2007; some of the exploited CVEs were identified as far back as 1999. Second, half of the CVEs that were publicly announced and exploited in 2014, were exploited within the first two weeks after the CVE announcement.

### Patching strategy:

Based on Verizon's findings, there are several things that can be immediately incorporated into your ongoing patch management process.

**Verify that old patches have been addressed.** The DBIR shows that focusing only on recently identified vulnerabilities leaves a large hole in your security posture. In light of this information, it would be valuable to do a comprehensive review of your total environment and deploy some of the older patches.

### **Don't forget about Zero Day and new CVEs.**

Unfortunately we can't only focus on older issues. As the

report showed, any announcement of vulnerabilities likely means exploits are on the way. If the vulnerability is public knowledge and is broadcast in security forums, you can bet hackers have the same information and will utilize it if given the chance. Find a way to prioritize older and newer CVEs to ensure both types are being addressed.

### **Continue to evaluate the effectiveness of your patching program**

– There are always challenges when running an effective patch management program but it can be a low cost initiative that can greatly increase your security posture. Self-evaluate your program and identify what challenges you

may have that prevent you from achieving the compliance rate you desire. Is it organizational issues such as needing more time or

dedicated staff to manage the process? Perhaps your change management process is too cumbersome to allow agile deployment of new patches. Identify the challenge, then document a plan to address the issue. This may be helpful in getting any resources or approvals that are needed to improve your compliance rate.

To comment on this or if you have any relating questions please email us at [security-alerts@nsoc.dir.texas.gov](mailto:security-alerts@nsoc.dir.texas.gov)

Jeremy Wilson

Network Security Operations  
Center Security Manager



**99.9%**  
OF THE EXPLOITED  
VULNERABILITIES WERE  
COMPROMISED MORE  
THAN ONE YEAR AFTER  
THE CVE WAS  
PUBLISHED.

# Information Security Officer Spotlight

## Arturo Montalvo, CISSP Information Security Officer The Office of the Attorney General

I grew up in Laredo, TX - where the IH-35 corridor meets the Texas/Mexican border. I studied at Texas A&M International University for my Bachelor of Business Administration in Management Information Systems. I started my security career at that university and I've been at the OAG for 3 ½ years – ISO for the Admin and Legal divisions since June.

### How did you come to the security field?

I was a computer whiz in high school – it was an engineering and technology magnet school so C++ and Java was part of the curriculum. I started making simple, non-malicious gag applications. One of them landed me in in-school suspension and in the eyes of the one of the district's IT directors. Fast forward a few years. I was a student in college, the IT director was now working there. I got a job in the university's IT department, studied for and took Microsoft certifications, and was quickly promoted. This time, I was hardening the student lab computers to prevent students doing what I was doing in high school. That got the attention of another director – the Information Security Officer. I started working on her team as an IT security analyst upon graduation. She was offered the ISO role at the OAG in Austin, and shortly after I joined her team again.

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

There's more focus on information security now – it's easier to explain what I do for a living to someone with all the news going around regarding data breaches.

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

My customers are everyone who has been authorized to read, enter, or update information by the owner of the information; to access an information resource in accordance with owner-defined controls and access rules. They include OAG employees, temporary employees, volunteers, interns, private providers of services, contractors and sub-contractors, vendors, auditors, consultants and representatives of other entities or agencies of state



government authorized to access OAG information resources. Yes, I totally copied that from our information security policy. Yes, you may edit this definition to your needs and use it as a template for your agency/university.

The most challenging area is finding the balance between security and functionality. The agency manages a wide variety of information – from public information to highly regulated data. If, for example, the agency wants to use a cloud service, it is my team's responsibility to define the appropriate controls for that data classification and educate the data owners on the residual risk. It's about enabling the business and reducing risk – reducing risk so that the agency can take other risks. Finding this balance is the most challenging area for me but the most rewarding.

### What do you like best about your job?

I like waking up with a purpose – what we do in this agency is amazing! This includes cracking down on human trafficking, arresting predators who commit crimes against children, investigating and prosecuting cases regarding Medicaid fraud, protecting consumers, and defending both state agencies and employees of Texas when they are sued – to name a few. I'm happy to be a small part of it and in helping our attorneys do great things.

### What would people never guess you do in your role?

My role usually consists of making and receiving calls to HR, General Counsel, the procurement division, other ISOs around the state, technical IT people, and basically everyone

throughout the agency. Communicating effectively is essential and usually consists between translating technical terms to non-technical terms and vice versa.

**What other career would you have liked to pursue?**

I would eventually want to be an IT auditor or consultant so that I can “drop the bomb and run!”

**Have you ever changed career paths?**

No

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

That’s classified.

**Tell us about your most proud accomplishment.**

Being one of the youngest ISOs at an agency this size.

**Top 3 life highlights?**

Born; TBD; TBD.

**What are your hobbies?**

Homebrew beer, cider, wine, and I’m trying to make kombucha. Bread making, cheese making – if it ferments, I want to have my hands on it. I’m an avid reader. Hitting the trails on my mountain bike.

**People would be surprised to know that you....**

are an award winning home brewer.

**Any favorite line from a movie?**

“All the power in the universe, and I am bound by the rules of the genie.” –Jafar Aladdin: The Return of Jafar.

**Are you messy or organized?**

I have an organized mess.

**What is your favorite Pokémon character?**

I just made that question up and added it here to see if anyone is paying attention. *(Yes, we saw that Arturo.)*

**Favorite travel spot?**

Most recently it was Barcelona, but anywhere in Europe is fine by me.

**What was the last book you read?**

Of Love and Other Demons by Gabriel Garcia Marquez

Last Read: The Five Dysfunctions of a Team: A Leadership Fable by Patrick Lencioni

**What radio station do you listen to?**

I usually listed to BBC World News on my way to work.

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

I would love to have a drink with Carl Sagan.

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

Food truck tacos.

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

Me at age 55 – to give my current self correction or direction.

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

Arturo’s Discourses on Beer, Love, and Life in the 21st Century: Volume One

**Describe what you were like at age 10.**

Disassembling various equipment to see how they worked – and with a surplus of screws.

**What is one thing you couldn’t live without?**

Calories.

**What is your hidden talent?**

I don’t know – it’s hidden to me.

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

Hay más tiempo que vida – Life is short, seize the moment (no, not YOLO)

**What would be your advice for a new security professional?**

Never stop learning! Read everything you can get your hands on. Make valid opinions, change them when you have better information. Network! Learn about your business, you are here to support them. Read your employer’s intranet site. Network!

The OAG is charged by the state constitution to defend the laws and constitution of Texas, represent the state in litigation, and approve public bond issues. There are nearly 2,000 references to the OAG in state laws.

# Program Updates

## Updates to the Archer Incidents Module

We recently released revisions to the Archer Incidents Module. These changes will help you and the NSOC team better communicate. Additionally it will help the NSOC team track the alerts they send you and help fine tune their tools and provide you with better alerts.

The first change is at the very top of the Incident page. There is a place to acknowledge that you have seen the alert from the NSOC. Click **Edit** at the top of the screen, and then check the **Acknowledgement of Alert from NSOC** box. This will change the **Status** field to **Alert Acknowledged and in Process**.

The screenshot displays the Archer Incidents Module interface for incident INC-1392. The 'Incident Progress' section shows the 'Acknowledgement of Alert from NSOC' checkbox checked. The 'Incident General Information' section shows the 'Status' field set to 'Alert Acknowledged and In Process'.

The second change is on the **Indicators of Compromise** tab. This provides the ability to show the source or destination coming from an internal or external IP address, and provides a structured way of storing the IP address.

The screenshot displays the 'Indicators of Compromise: Add New Record' form. The 'General Information' section includes the following fields:

- Tracking ID:
- Source or Destination?:  Destination  Source
- Internal or External?:  External IP  Organization IP
- Domain:
- Please use either IP 4 or IP 6 depending on which is applicable
- IP 4: [ ] . [ ] . [ ] . [ ]
- IP 6: [ ] : [ ] : [ ] : [ ] : [ ] : [ ] : [ ] : [ ]
- Primary Function of Affected System:
- Users Affected:

Additionally, we have given you the ability to see some statewide roll-up information on the monthly incident dashboard. Simply select **Monthly Incident Roll-Up Reporting** on the Dashboard drop down menu and you will see your agency totals and then the totals for the state, and then totals by agency size. Here's an example screenshot:

The screenshot shows the 'Monthly Incident Reporting System' dashboard. At the top, there is a navigation bar with 'Dashboard: Monthly Incident Roll-Up Reporting' and a welcome message 'Welcome, Smith Sally'. Below this, there are two tabs: 'Monthly Incident Reporting System' and 'Confidentiality Statement'. The main content area features a title 'Monthly Incident Reporting System' and a brief description: 'All security incidents submitted during the prior month in the Archer system will roll up into the agency's monthly record. Agencies can add additional incident occurrence information to get a total records for the month. Monthly Incident Reporting has been streamlined to minimize effort while gathering important details.' To the right of the title is a red confidentiality warning: 'The information found in this system is confidential. Given the file system as confidential. Please mark printed materials from this system as confidential. Please mark printed materials from this system as confidential. Please mark printed materials from this system as confidential.' Below the title is a section titled 'Monthly Incident Reporting Records Current Month' which contains a table with the following data:

Tracking ID	Organization Name	Reporting Month	Reporting Period	Environmental Total	Error Total	Hacking Total	Malware Total	Misuse Total	Physical Total	Social Engineering Total
234760	State Agency for Archer	June	6-2015	0	0	0	0	0	0	0
229366	State of Texas Rollup Record	June	6-2015	3	16	21	253	7	9	459
229036	State of Texas Incident Rollup-Small	June	6-2015	3	0	2	29	0	1	7
229028	State of Texas Incident Rollup-Large	June	6-2015	0	8	10	137	3	4	436
229025	State of Texas Incident Rollup-Medium	June	6-2015	0	8	9	87	4	4	16

Page 1 of 1 (5 records)

As always, if you have any questions, please contact us at [GRC@DIR.Texas.gov](mailto:GRC@DIR.Texas.gov).

# Insight from our Texas CISO

Over the past several months the Office of the CISO has undergone several changes. We discussed my role as the CISO, but my job would be impossible if it was not for the incredible team I work with. This month, I'd like to highlight the team and let you know of some of the changes we have undergone in the office.

*Claudia Escobar* became the Deputy CISO in September of this year. She currently oversees daily operations and activities of the agency's statewide cybersecurity and information security program. Claudia started as a network specialist over 20 years ago. She has experience in private and public sectors. Prior to joining the team at the Texas Department of Information Resources (DIR), Claudia served as the Information Security Officer for the Administrative and Legal division at the Office of the Attorney General. She also served as the Information Security Officer and Director of IT services at Texas A&M International University. Claudia holds a bachelor's degree in Computer Science and is a Certified Information Systems Security Professional (CISSP).



*Eddie Block*  
CISO, State of Texas

*Nancy Rainosek* has over 30 years of IT experience in private sector consulting and Texas state government. She leads the extensive Governance, Risk and Compliance (GRC) program. The Archer incident reporting, risk assessment, and security plan modules would not exist if it wasn't for her guidance. Prior to joining DIR, Nancy served as the deputy Chief Information Security Officer and the Manager of Enterprise Security Operations for the Health and Human Services Commission. She also served as an IT Audit Manager and Information Resources Manager at the State Auditor's Office.

*Jeff Rogers* is the Security Program Manager for the Data Center Services at DIR since June 2014. In this role Jeff is constantly seeking ways to continue to improve the security posture for and maturity levels of the State's consolidated data center and further the mission of the Chief Information Security Office. Jeff has bachelor degrees from Texas A&M University and the University of Maryland. He also has an Information Assurance Graduate Certificate from the NSA Center of Excellence at University of Dallas, has completed numerous graduate courses at the National Defense University, and has held a CISSP certification since 2006. Jeff is a military veteran and brings over 15 years of IT and Cybersecurity management experience in corporate and federal spaces.

*Suzi Hilliard* joined DIR in December 2014 as the Statewide Information Security Services Program Delivery Lead. She has 15 years of experience in the IT world, almost ten of those working in information security with the state of Texas. With a focus on security management, policies, and user awareness, Suzi strives to continuously improve security programs in state government. Before joining DIR, Suzi worked as a security analyst for both the Texas Attorney General's Office in the Child Support Division, and for the Department of State Health Services. Suzi has a Bachelor of Arts in Communications from St. Edward's University, and holds a CISSP certification.

*Hannah Folgate* is a Marketing Specialist working at DIR since July 2014. Hannah develops communications and publications for the CISO. In addition, she assists the Texas Cybersecurity Coordinator and Texas Cybersecurity Council in their efforts to promote cybersecurity awareness and education. A recent graduate of Concordia University Texas, Hannah majored in public relations and marketing.

Without this team and the experience they bring, both in the public and private sectors and through the ranks of IT from technical, ISO, and IRM roles, we would not be able to build the type of program that the State of Texas deserves. I am humbled and inspired that they serve alongside me.

*Eddie Block*  
CISO, State of Texas

# Events

---

## 2015 Save the Dates

- [LASCON 2015](#), October 19 – 22
- [Dallas Secure World](#), October 28 – 29, 2015
- [BSides Dallas](#), November 7
- [Austin ISSA Brings Chris Hadnagy to Austin](#), December 10 – 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 can employ 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](mailto:education@austinissa.org)

## Lonestar Application Security Conference

October 20–23, 2015

Austin, Texas - Norris Conference Center

Join us for the OWASP sponsored Lonestar Application Security Conference on October 20–23, 2015. LASCON offers focused training and discussions for developers, operations, security managers and anyone trying to integrate security into the new developing world we find ourselves. The training is practical and focuses on subjects including:

- Managing Application Security Risk
- Secure Development in Node.js
- Creating and Automating your own AppSec Pipeline
- OWASP Top 10 and Defensive Programming for JavaScript

Register for conference today! Limited seating is available.



Feedback, comments, stories, etc.  
[DIRSecurity@dir.texas.gov](mailto:DIRSecurity@dir.texas.gov)



Office of the  
CHIEF INFORMATION  
SECURITY OFFICER  
State of Texas