

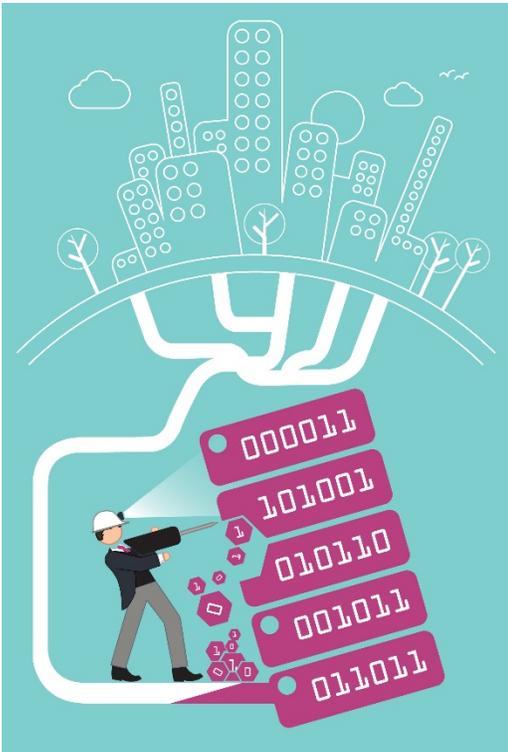


July FY2015 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV



How can we help?

Are you familiar with the Security Services OCISO offers? Please send us an email.



Contents

Monthly Article

Time Marches On	2
Network Security Operations Center Update	3
Our State ISO Spotlight	
Kent Dyer	4-5
Texas Information Security Program Updates	
InfoSec Academy	6
Archer GRC Portal	7
From our State CISO	8
Events	9

Time Marches on

Back in 2003, camera phones were brand new and the cause of great controversy; Apple launched iTunes; national Do-Not-Call lists started limiting those annoying telemarketer calls. And Microsoft launched Server 2003.

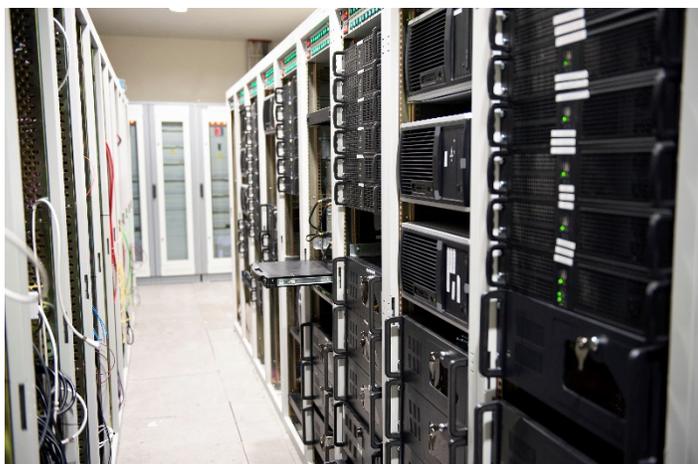
Twelve years later, camera phones are standard and expected to be better than regular digital cameras. iTunes is one of the most popular sources for downloadable content – music, movies, TV shows, and more. And although telemarketers are still on the loose, Microsoft Server 2003 will reach End-Of-Life (EOL) in mid-July.

Although state agencies are not always able to keep up with the technology curve, ensuring that EOL equipment is taken out of the infrastructure is extremely important. EOL software or equipment no longer receives security updates or support from the manufacturer – so they become fair game for hackers and evildoers.

As July looms closer, it is important to ensure the risks of leaving systems on Server 2003 are worth the possibility of a breach. The data owners, decision makers, management, and budget personnel should all be involved in the planning and execution of Microsoft Server 2003 phase out.

If you have questions regarding the Microsoft Server 2003 EOL, there are several webinars and articles online. BrightTalk has archived a webinar that provides some good information. [Click here to view the webinar.](#)

If you have other questions, contact DIRSecurity@dir.texas.gov.



Network Security Operations Center (NSOC)

In previous issues, we have identified four capabilities as being crucial to the NSOC's mission of supporting the state's and our customer's security programs. These capabilities are detection, mitigation, communication, and prediction. This month we will discuss two of these capabilities, detection and communication, and how we are working to enhance those capabilities.

Detection

The NSOC uses multiple Intrusion Detection Systems (IDS) to give us the best picture into the state's network traffic. However, we routinely perform Proofs of Concepts (POC) to determine if new technologies would benefit our customers. In performing these POCs, we have identified some new technologies that are enabling us to more easily see and catch things that previously may have gone undetected. With new technology implementation, there can be some growing pains – tuning these monitoring devices can be tedious and time consuming. The tuning is necessary to ensure that DIR customers are alerted on valid events.

Getting feedback from our customers can help us to more quickly and easily tune these devices. The DIR NSOC alone cannot determine if an alert is valid or a false positive. We are asking our customers to help us through this process. When an alert is sent out, sending back a response letting us know if the alert is valid or if it is a false positive can help us to tune these appliances more quickly and efficiently and help to make sure that the alerting system is accurate.

If you have questions on toolsets or architecture or need help on a specific alert that is sent to you, contact the NSOC via our distribution list at security-alerts@nsoc.dir.texas.gov.

Communication

Through our internet service providers, we provide Distributed Denial-of-Service (DDoS) monitoring, protection, and mitigation on our network. Although most of the monitoring activity happens behind the scenes and does not affect our customers, there are

times when our customers are affected. When this happens, the NSOC will provide an executive summary report of the activity and response to the affected customers.

The executive report will be sent to the affected Chief Information Security Officer/Information Security Officer of the affected organization and can be forwarded to those with a need to know in their organization. The DDoS executive report will be one to two pages in length and will summarize the details of the attack and the response actions taken by the NSOC and its providers. The report will contain a graphical view of the attack traffic that was mitigated. The report will also contain a timeline of the event including:

- Time of notification of the attack
- Time our response (investigation) began
- Time mitigation was initiated
- Time of notifications or escalations within DIR or to the targeted agency
- Conclusion of the attack
- Time of suspension of the mitigation

The monitoring and protection currently in place is at a threshold deemed appropriate for the state. If we see an attack against the entire state, a portion of the state's IP space, or even just a specific target, we will mitigate that attack. That threshold is constantly evaluated, and behavior monitoring is performed to ensure that we don't mitigate legitimate traffic. A targeted attack against one of your critical hosts or applications could be at a low enough level that the NSOC may not get notified. If you are an Internet customer of DIR and you suspect that you are experiencing a DDoS

attack, please call 512-633-6050 or 888-839-6762, or email us at security-alerts@nsoc.dir.texas.gov. We can mitigate targeted attacks if we are notified by you even if they do not trip the monitoring and mitigation thresholds.



SHRED DAY SUCCESS!

The DIR NSOC had a successful Shred Day event in May. The NSOC securely destroyed 1692 hard drives and 4316 other devices (tapes, CDs, phones, etc.). Almost two tons of recyclables were diverted from landfills! Our next NSOC Shred Day will be in October and will be free to our customers.

If you have questions about the NSOC or Shred Day events, please contact Jeremy Wilson. Stay safe and cool, and enjoy your summer!

Jeremy A. Wilson
DIR Security Operations Center Manager

Information Security Officer Spotlight

Kent Dyer

Information Security Officer and -SANS
GSLC, NSA IAM & IEM, CsS, SCP

I started working for the state in 1993, as the Asst. Automation Coordinator at the MHMR Corpus Christi State School. I moved to Austin in 2000 as an Enterprise Network Consultant for MHMR Enterprise Network Services. In 2004 when House Bill 2292 broke MHMR up – I went to the private sector for a few years, and then came back to the state at HHSC Enterprise Security. I was then the CISO at TWC for about 8 years before starting my current gig at TDLR. All told, I have going on 22 years with the State of Texas, and I'm very proud of that fact.

How did you come to the security field?

At MHMR, I introduced a consolidated, managed antivirus system to the entire enterprise, which I managed from the Winters Complex here in Austin. I became known for blocking and killing viruses. There were many late nights – I recall logging into Exchange servers at 24 locations and removing the infected messages from the message queues. I continued managing networks, but always had protection in mind. When I went to HHSC, I went straight to Information Security, and never looked back.

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

It has significantly matured. No longer are we just IT staff, killing viruses, we are professionals trained to manage risk, vulnerabilities, ensure that our agencies are in compliance with regulations, and safeguard information and privacy.

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

Ultimately, my customers are the citizens of Texas that have entrusted their information to TDLR, and I try my hardest to keep that at the forefront of my thoughts, and to impress that upon all agency staff.

My biggest challenge is that I want to accomplish so much more than I can currently do. We are going to hire some staff to help with the security program, so that's a really great thing.



How did you learn about TDLR?

When our IT Director at TWC moved to TDLR, and I looked it up to see what it's all about.

What do you like best about your job?

Having the full support and backing of TDLR's Executive Management for the Information Security program. They truly understand and are on board.

What would people never guess you do in your role?

I actually write and produce my own Information Security CBT classes.

What other career would you have liked to pursue?

I've always wanted to be an architect and homebuilder. My Grandfather was a carpenter and homebuilder for over 50 years. My brother has been a builder for years – it's in my blood. I love to see a building rise up from the ground.

Have you ever changed career paths?

I have thought about it at checkpoints in my career. But I find it more compelling every day. I believe I made the right choice for my career.

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

Adult Attention Deficit Disorder. I have to keep lists, calendars, and a whiteboard handy. I'll never win, but ADD won't either.

Tell us about your most proud accomplishment.

Getting published in Government Computer News twice.

Where did you grow up?

Corpus Christi, TX. (I'm not sure I ever really grew up...)

Do you have family in Austin?

My mom lives nearby in Pflugerville, and my brother lives in Briarcliff, in a home that was the site of Willie Nelson's 4th of July picnics in 1979 and 1980. (The stage was in his backyard on the golf course.)

What are your hobbies?

There are so many... electronics, photography, flying quadcopters, woodworking, reading, writing, fishing, metal detecting, rock hounding and most recently, 3D printing. I guess my hobby is having hobbies.

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

I'm a huge space junkie, and collection of astronaut autobiographies signed by astronauts, including Alan Shepard, first American in space. I also have 4 cats.

Any favorite line from a movie?

"Get busy living, or get busy dying." Andy Dufresne – Shawshank Redemption

Are you messy or organized?

MeSsY!!!!

Favorite travel spot?

Lake Kabekona, MN – a family cabin on the water far away from civilization.

What was the last book you read?

That's hard to answer – it's a Kindle. On it you'll find The Martian by Andy Wier, and Ready Player One by Austin's Ernest Cline.

What CD do you have in your car?

The entire catalog from Barenaked Ladies is on the hard drive in my truck's stereo, along with the soundtracks from Shawshank Redemption and Battlestar Galactica. I may or may not have Josh Groban music on there as well. I'll neither confirm nor deny.

Top 3 life highlights?

Tied for top – birth of my 2 sons, third: marrying my wife.

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

Neil Armstrong.

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

Dad's meatloaf, Mom's potato salad, sweet tea, and a salad.

Least favorite food?

Liver and onions.

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

Hiro Nakamura, from the TV Show, Heroes. I'd freeze time and catch up on sleep and my Netflix queue.

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

Distracted Geek. ©2015

Describe what you were like at age 10.

I was a quiet, shy, nerdy kid, with my nose always either buried in a book or watching TV.

What is one thing you couldn't live without?

Books.

What is your hidden talent?

Soldering. I swore for years that I was no good at it, and had a project about 2 years ago to do – so I tried, and can solder with amazing results. Since then, I build electronic projects for fun. (If you're wondering, a GOOD iron and flux are the answer.)

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

Just protect the information. That's what is important.

What would be your advice for a new security professional?

Consider who the true owner is of the information you're tasked with safeguarding. Always think about them, act appropriately, and do everything necessary to protect their information. Think, Act, Protect.

Program Updates

Texas InfoSec Academy

Texas Security Policy & Assurance Course

Five sessions of the Texas Security Policy & Assurance (TXSPA) course were offered this spring with the final session offered during the Information Security Forum in May. The course will be available online in mid to late August and you may enroll in it now. If you enroll in the TXSPA online course, you will receive an email notification when it is available.

Enrollment in this course is a prerequisite for taking any of the certification preparation courses, such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), and Certified Information Systems Auditor (CISA). The CISSP and the CEH are currently available, and CISA and CISM will be available soon.

*You must also complete the Certified Information Systems Security Officer course and one soft skills class in order to enroll in a certification prep course.

Continuing Education Credits

You can earn continuing education units for participating in InfoSec Security classes. The number of hours you can earn varies by course. The following table gives an overview:

Certified Security Sentinel	16 Hours
Certified Vulnerability Assessor	16 Hours
Certified Information Systems Security Officer	40 Hours
Top 20 Information Systems Controls IS20	24 Hours
Certified Security Leadership Officer	40 Hours

Certified Incident Handling Engineer	40 Hours
Certified Digital Forensics Examiner	40 Hours
Certified Network Forensics Examiner	40 Hours
Certified Disaster Recovery Engineer	32 Hours
Certified Secure Web Application Engineer	32 Hours
Certified Penetration Testing Engineer	40 Hours
Certified Penetration Testing Consultant	32 Hours

CSS and CISSO Courses and Exam Vouchers

Several students who are enrolled in these courses have not yet taken the exam. We will be contacting those students to see if you have any questions or need any assistance. If you are not able to continue the program, please contact infosecacademy@dir.texas.gov.

For all security courses, each student gets two attempts to pass the exam. To request exam vouchers for security courses, email infosecacademy@dir.texas.gov.

Recorded Sessions

To access the previously recorded online sessions, log in to infosecacademy.dir.texas.gov and click on the link to the InfoSec Academy Forum (on the right side of the page). Then click on the link that says, "View Prior Recorded Q & A sessions."

Do you have a seat in the academy? Email us to find your access.



Archer Incidents News

The DIR Network Security Operations Center (NSOC) has been using the Archer Incident Reporting system to send agencies suspicious events that may be indicative of a security incident. The email will look like this:



Click on the INC-XXX link to log in to Archer. Once you authenticate to the system, you will be taken directly to the event. Click on the "Indicators of Compromise" tab to view the source and destination IP addresses and other pertinent information. Please ensure that as you work this incident, you indicate in the *Incident Confirmation* field if this is a confirmed incident. Otherwise, indicate how you classify this activity. This enables the NSOC to measure the performance of the various tools they use to help you protect your organization.

As you work on this event, if you indicate it as confirmed and record the other pertinent information, it will automatically be included on your Monthly Incident Report.

Insight from our Texas CISO

As you read this edition of the DIR Cybersecurity Insight Newsletter, I will likely be somewhere between 7 – 12,500 feet above sea level in Northern New Mexico. This is about mindset.

Like many of us, I have so many roles in my life, aside from my roles as the CISO and Cybersecurity Coordinator for the state, I also have the role of assistant scout master for Troop 159 in north Austin. So for two weeks this summer, I will be hiking an 81-mile circuit on the Philmont Scout Ranch in Cimarron, New Mexico. This has made me think and found a lot of similitudes between my roles.

I have found similar elements of building and developing a security program laid out in the planning required for this trip.

For this trip I'm not setting the path. The youth chose the activities for our hike. They have decided to go rock climbing, horseback riding, and black powder shooting. Likewise, many of us don't set the path for projects in our organizations. While some security professionals may be involved in planning discussions, the business of our organization ultimately determines our strategic goals. We are there to ensure that those goals can be executed without sacrificing the confidentiality, integrity, or availability of our data or systems. In the same way, I'm on the trek to make sure that the youth can climb, ride, and shoot safely.

With the waypoints of our trek laid out, we set our path. I'm pretty good with land navigation, but I'm not the one carrying the map. One of the youth is in charge of getting our team from point A to point B each day. I have to trust the navigator not to turn our 81-mile trek into a 100+ mile slog. My job is to make sure that our navigator has a map and compass and is trained to use them. Similarly, we have to ensure that the people working on our IT systems, whether our team, other agency employees, contractors, or vendors, understand the path and tools.

Questions to consider:

- Are we all working from the same map and orientation? (clear goals and mission oriented)
- Does everyone with need-to-know understand the agency or institution's security plan? (education and awareness)
- Do our people have the right tools and training for the job? (workforce)
- What happens if our primary navigator gets hurt or sick? Can someone pick up his plan and continue down the path? (disaster recovery and incident response plan)

Whether a security analyst, executive staff, or an agency employee, our role is to ensure that we orient our people and make sure they have the tools they need to protect the data and systems entrusted to them.

Finally, I have to trust our navigator to do his job, just like we have to trust our security teams. I am thankful the team I have around me is outstanding, and I know they will be responsive and capable in my absence.



Eddie Block
CISO, State of Texas

Eddie Block
CISO, State of Texas

Events

Training and Conferences around the State

Monthly Security Program Webinar

Selecting the Right Identity Governance and Administration tool for the Job!

Date: May 12, 2015 at 2:00 PM CDT.

Time: 2:00 pm CDT

Register now!

2015 Save the Dates

- NSA Information Assurance Directorate's (IAD) Information Assurance Symposium (IAS): June 29 – July 1 Washington, D.C.
- Blackhat USA, August 1 – 6
- TASSCC Annual Conference, August 2 – 5; La Cantera Resort, San Antonio
- BSides Las Vegas, August 5 – 6
- Defcon 23 August 6 – 9
- LASCON 2015, October 19 – 22:
- Dallas Secure World, October 28 – 29, 2015

Do you know our team?



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



Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas