THE DIR CYBERSECURITY INSIGHT

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

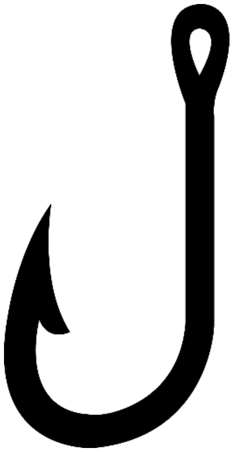
Gone Phishing by MS-ISAC

Defend yourself against phishing scams by utilizing a spam filter, keeping systems patched and anti-virus software up to date. The second line of defense against phishing is you. If you are vigilant and watch for telltale signs of a phishing email, you can minimize your risk of falling for one. Signs of a potential phishing attempt include messages from companies you don't have accounts with, spelling mistakes, messages from the wrong email address (e.g. info@yourbank.fakewebsite.com instead of info@yourbank.com), generic greetings (e.g. "Dear user" instead of your name) and unexpected messages with a sense of urgency designed to prompt you into responding quickly without checking the facts. "Resume" and "Unpaid Invoice" are popular attachments used in phishing campaigns.

Protect yourself and your family:

- Be suspicious of unsolicited emails, text messages and phone call. Use discretion when providing information to unsolicited phone calls and ***never*** provide sensitive personal information via email.
- If you want to verify a suspicious email, contact the organization directly with a known phone number. Do not call the number provided in the email. Have the company send you something through the US mail (which scammers won't do).
- Only open an email attachment if you are expecting it and know what it contains. Be cautious about container files, such as .zip files, as malicious content could be packed inside.
- Visit websites by typing the address into the address bar. Do not follow links embedded in an unsolicited email.
- Use discretion when posting personal information on social media. This information is a treasure-trove to spear phishers who will use it to feign trustworthiness.
- Keep all of your software patched and up-to-date. Home users should have the auto update feature enabled.
- Keep your antivirus software up-to-date to detect and disable malicious programs, such as spyware or backdoor Trojans, which may be included in phishing emails.

Brought to you by MS-ISAC. Read more articles here.



CONTENTS

Network Security Operations Center (NSOC)

Take a moment to remind yourself of the importance of addressing legacy systems and applications in your environment. This issue isn't new to security professionals but is still of a critical nature. The NSOC has been responding to numerous security incidents in the state and has identified several environments with outdated and unsupported systems and applications. This issue poses a substantial risk not just to your organization but to your customers and business partners. Running outdated and unsupported operating systems and applications can leave you susceptible to any number of attacks. The recommendation will always be to upgrade and then patch, patch, patch. There may be a number of reasons organizations are not upgrading or patching legacy systems. Business stakeholders may consider the upgrade or replacement to be too expensive. Perhaps there is a fear that any attempt to upgrade will interfere with a critical service offering. It is also important to inform your stakeholders of the impacts of not upgrading or fixing legacy systems. This may cost them in the form of lost or inefficient use of limited resources, reputational damage or financially through the cost recovery following a serious data breach. As security professionals, you are in a position to help the decision makers see and understand these hidden costs.

There is always a lot of buzz in the security business around new security tools. Your toolset should be an important part of your security program. However, if you have not completed a firm inventory of your equipment and data, how can you truly defend your systems and information? Your time and money would be well spent making sure you understand all of your systems and data. Put plans in place to update any legacy systems and maintain a good patch management program before investments are made in other areas. To summarize, assess and present the risk to stakeholders, then manage the risk by putting plans in place to update and upgrade as soon as possible.

Learn more on legacy systems and how to address the risk they pose to you and your data.

I can be reached at Jeremy.wilson@dir.texas.gov.

SPECTRIM

Formerly known as Archer, the Statewide Portal for Enterprise Cybersecurity Threat Risk and Incident Management or SPECTRIM, was adopted April 2016.

Are you planning to request Cybersecurity Funding in your FY 2018-2019 LAR? If so, it is important that you enter your 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 Archer online application. You can find additional information including a webinar recording that presented this function at http://dir.texas.gov/View-Resources/Pages/Content.aspx?id=54

Data Center Services

Browsers and Certificates

As the cybersecurity discipline of encryption evolves, encryption management is required for those who are serving websites and/or conducting e-commerce. Modern web browsers try to keep their users safe and send notifications when they might be straying into potentially dangerous areas. One of these areas is the gauging of risk of the settings and certificates that the websites uses. The major web browsers track certificate details such as who issued them, encryption algorithm used and protocol used.

Customer perspective should drive your decision on certificate choice. A website built for customers or public consumption is representative of an organization. If issues are presented to a webpage visitor, it does not make a good first impression if their browser warns of something potentially unsafe. Properly managing and using certificates issued by a Certificate Authority (CA) on these systems will more accurately represent an organization's website.

Secure Socket Layer (SSL) 2.0 and 3.0 have both been identified as insecure with most encryption algorithms. Transport Layer Security (TLS) 1.2 is the current standard although version 1.3 is in draft status. Additionally, web browsers are phasing out and deprecating SHA-1 certificate acceptance through their browser versioning in announced roadmap planning. Some CA's will allow you to switch any SHA-1 certificates for SHA-2 should you have any in place. The browsers are forcing these changes at the pace they see fit with their versioning and deprecation plans so IT and security need to make sure they are planning for these changes. This is just another area where currency is a huge factor in proper maintenance of a secure environment. If you are not using secure algorithms and protocols you are placing your organization and your customers at risk.

In January, NIST released revision 4 of Special Publication 800-57, Part 1. This series of Recommendations of Key Management are important for any application development projects and can serve this area of a computer security program as well

Controled Penetration Tests

Something our pen test team sees time and time again is the use of bad passwords. With data breaches becoming a common occurrence, using stronger passwords or implementing a stronger password policy becomes necessary. Some of the most commonly used passwords are: password, 123456, abc123, qwerty, letmein, iloveyou (variant 1lov3you), incorrect (variant 1ncorr3ct). Other examples include pet names, numeric values of family member birthdays or months of the year.

So why do we see bad passwords being used? On the technology-side, domains and password management systems may allow it by implementing poor password policies. On the human-side, users want to tread the path of least resistance. If they must come up with a password with uppercase, lowercase and a number, then something like 'Password1' is convenient.

So what are some solutions?

For users:

- **Use a password generator**
- **Use a password with a good-sized minimum of characters**.
- **Use phrases as passwords rather than common words**.
- **Use private password managers.** Software like LastPass, Dashlane or Password Safe keep a database of accounts and password information. ****Keep in mind** that no system is invulnerable, as LastPass was compromised in 2015**.
- (If you absolutely must have them written down) **Use encryption software**. Programs like Folder Lock, TrueCrypt, AxCrypt or 7Zip encrypt those text/doc/xls files that list your passwords.

For agencies:

- **Implement a stronger password policy**. This includes setting up password with
  - **Minimum character lengths**
  - **Requiring the use of special symbols/characters**
  - **Setting expiration dates**
  - **Minimum/Maximum password age**
  - **Enforcing password history**

Information Security Officer Spotlight

Kevin Kjosa, CISSP
Information Security Operations Officer
The University of Texas at San Antonio

I started out as an officer in the U.S. Army. After leaving the Army, I worked for Thomson Inc. (Formerly RCA Corporation) global security office. I've been in information security ever since then. I began working with UTSA at the Center for Infrastructure Assurance and Security (CIAS) in 2008.

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

The profession has become more formal and diversified. The threats have changed or rather the threats have adapted.

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

Our customers are staff, faculty and students. We find it challenging to balance expectations of our customers with security requirements.

What do you like best of your job?

UTSA has a vibrant culture which makes working with our customers interesting.

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

I recall organizing state and local cyber exercises during my time with the CIAS. We put a lot of pressure on ourselves to maximize attendance. We relied on local representatives invite and organize participants. In many communities, things worked out and we'd max out the exercise. There were a few times where - at the eleventh hour - I would resort to cold-calling local officials and business leaders in communities and raise participation to maximum capacity.

But I enjoy talking to people a lot. I found it fun.

Tell us about your most proud accomplishment.

I am most proud of my three children.

Top 3 life highlights.

Taking a commission with the Army

Finishing graduate school

Becoming a father

What are you hobbies?

In what little free time I have, I will go for a run.

Any favorite line from a movie?

"You keep using that word. I do not think it means what you think it means." - The Princess Bride.

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

Ridley Scott. We'll discuss sci-fi movie plots and I'll ask for much-needed explanations.

What is one thing you couldn't live without?

I've heard there are people who do not drink coffee. They must have super powers.

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

Learn the business first and listen. Read and understand all the existing policies. Validate your coworkers.

What would be your advice for a new security professional?

Learn the business first and listen. Read and understand all the existing policies. Validate your coworkers.

OCISO Corner – Getting to Know the Team

Claudia Escobar
Deputy Chief Information Security Officer
Department of Information Resources

What is your responsibility in DIR and with the State?

I currently oversee daily operations and activities of the statewide cybersecurity program. I work with the OCISO team to help establish appropriate governance for information security strategies, policies and procedures. I also work with the State CISO developing plans, standards, and guidelines to address new security technology issues and trends. I coordinate state inter-agency security communication and information sharing as well as federal and state information sharing and collaboration for cybersecurity response.

When and where did you start your career?

I started my career working as a technician for a startup company in 1993 in Mexico. We were building and selling computers, installing networks and cabling, repairing printers, everything! I became their general manager at the age of 20. Days were very long but very fast paced. As a result, we became one of the two top companies in the market.

Why the security field?

When I was setting up networks, everything started changing with users and roles for the users, I started working with firewalls, routers, etc. Network security was a natural evolution of the work I was doing at the time.

What is your personal back ground?

I was born and raised in Mexico, however, travels broadened my perspective tremendously. I met my husband in 1999 at the SXSW festival. We now we have three kids - two boys and a girl, who are all very unique little people and I am fortunate to learn from them every day.

What did you want to be when you grew up?

I wanted to be a lawyer, but then I watched Star Wars and was curious about how the ship operated. I was fascinated with buttons and electronic panels so I started fixing (or breaking stuff at home) and my interest shifted.

What is the greatest lesson you have learned?

Finish with the problems, don't let the problems finish with you. Do it right the first time. Doing your best since the beginning will save you a lot of time and heartache in the end.

What do you want your legacy to be?

I love when my kids say that I am a funny, happy, sweet mom, and I think that is the most important thing for them to remember about me, although I am pretty sure they will also remember some of my beliefs:

- If you are waiting for the perfect moment, know that it is here now. You need to take risks and make decisions.
- Some people think they have a passion. For me, you may have 500 passions. 500 things that are your "purpose".
- A passion is a theory. Now you have to test your theory and the world is your laboratory. Construct the experiment that will test your theory, then test and test and test and tweak and test more.

Do you have a favorite hobby or pastime?

I can't say that I have just one hobby or pastime. Music is part of my life; the ACL music festival has become a tradition for my family. Kayaking, biking, writing, working out, meditation--these are just some of the things that I use to balance my soul.

What do you like best about working at DIR?

It is very gratifying to serve the state of Texas by helping agencies and higher education institutions elevate their information security programs. I enjoy working with people that care about people.

.Insight from our Texas CISO

Eddie Block
CISO, State of Texas

There are many things that get better with age; jazz, wine, cast iron pans and blue jeans come to mind. However, some things just don't stand the test of time; milk, memory, something else that I forgot and computers.

Legacy computer systems are an issue that many in the information security community see as a significant risk. Support for Windows XP ended April 8, 2014. This means it has been more than two years since a security patch has been available. Windows Server 2003 support ended on July 14, 2015. Legacy systems affect more than just Microsoft Oss. Red Hat Enterprise Linux 4, FreeBSD 8 and any version of MacOS below 10.8 are all unsupported. These systems will never see another security patch

How many users still have outdated, unsupported systems in production? According the legacy systems study it is a significant number. As a state, we have built a technology debt of legacy systems. These systems often hold confidential data, personally identifiable information and other regulated data. A breach of these systems could prove costly to address.

Many agencies get caught in an increasingly risky cycle with regards to legacy systems. Applications that have long since fallen out of support rely on unsupported libraries (Microsoft Active Server Pages comes to mind), which in turn rely on outdated operating systems.

Coding or procuring a new application means changing the underlying operating system, hardware and potentially finding staff that understand both the old and new development environment. It can be an overwhelming undertaking. But you must also consider the constantly evolving threat environment. At DIR, we have received multiple security events that originated on old, legacy, out-of-support operating systems or applications. The farther away a systems gets from the end of support date, the greater the risk.

In the 84th Legislative session, the legislature tasked DIR with prioritizing legacy and cybersecurity projects that will be proposed by agencies in the 85th session. The fact that we have been asked to prioritize these projects for the LBB shows me that there is an understanding that the technology debt must be addressed.

Over the next several months, DIR will use information supplied in our SPECTRIM tool to assess the legacy and cybersecurity projects that agencies will submit for funding. While it is unlikely all of the projects will be funded, we must look at this as the beginning of rebuilding the infrastructure that provides citizen services in a resilient and secure manner.

Eddie Block
CISO, State of Texas

Events

2016 Save the Dates

- DIRConnect: May 25, Palmer Events Center

ISF Follow Up

Presentations from the 2016 ISF are now available. CLICK HERE TO VIEW THE PRESENTATIONS.