ISSA Information Systems Security Association Colorado Springs Chapter
WWW.ISSA-COS.ORG

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 9 SEPTEMBER 2019

Colorado Springs, Colorado

Peak Cyber Symposium Occurring

ISSA-COS Members,

If it's September than it must be time for the **Peak Cyber** symposium! As you read this newsletter, the symposium will be wrapping up on another successful year of keynote speakers, amazing presentations, numerous training sessions, and one incredible Capture-the-Flag (CTF) challenge. By all accounts, the Peak Cyber symposium has become one of the largest annual Cybersecurity events in all of Colorado Springs. This year alone, 100+ people participated in the CTF challenge sponsored and facilitated by **Splunk>**. This represents a **4-fold increase** in participation compared to last year! Overall attendance for the symposium pushed 450 people making this year the largest event in recent years. **THANK YOU** to all our direct sponsors (**Murray Security Services, Handshake Leadership, Splunk>, AWS, and Jacobs**), community partners (**COS Chamber & EDC, SBDC, NCC, AFCEA-RMC, (ISC)2 – PP, PPCC, and ERAU**), chapter members, and volunteers for helping make this event such a great one!

Also occurring in September is the second annual offering of the ISSA-COS **Security + Review**. The reviews are scheduled for the following Saturdays: **9/14, 9/21, and 9/28** at CTU from 8:00 AM – 4:00 PM. The fee is only $50 and is **open to both members and non-members** so, sign-up, bring a friend, and get ready to pass that exam!! **Register at www.issa-cos.org**.

Looking back at August, our chapter enjoyed dinner and lunch presentations from **Mr. Thomas Hallewell**; special guest and Director of Programs from the ISSA Washington DC chapter. Mr. Hallewell's presentations on "*Fail Secure: 23 Ways to Undermine you Security Program*" were very well received and gave everyone quite a few chuckles. For our mini seminar, **Mr. Justin Whitehead**, Founder and CEO of Digital Silence presented: "*SO THERE I WAS – A Walk Through the Life of a Red Teamer*." The mini seminar included a hands-on "Cyber Range" experience from our very own Healthcare Special Interest Group (SIG) Leader **Mr. Dennis Schorn**. Together, these gentlemen "rocked the house" and provided folks with an excellent training experience. **THANK YOU**, guest speakers, for contributing to the professional development of our members!

(Continued on page 4)

A Note From Our President

By Mr. Ernest Campos

I Visited 47 Sites. Hundreds of Trackers Followed Me.

By Farhad Manjoo, The New York Times, August 23, 2019

A lot of entrepreneurs have "a moment". A moment that makes them realise they're on to something.

Earlier this year, an editor working on The Times's Privacy Project asked me whether I'd be interested in having all my digital activity tracked, examined in meticulous detail and then published — you know, for journalism. "Hahaha," I said, and then I think I made an "at least buy me dinner first" joke, but it turned out he was serious. What could I say? I'm new here, I like to help, and, conveniently, I have nothing whatsoever at all to hide.

"Even when companies don't have an ID to track me, they can use signals from my computer to guess who I am across sites."

Like a colonoscopy, the project involved some special prep. I had to install a version of the Firefox web browser that was created by privacy researchers to monitor how websites track users' data. For several days this spring, I lived my life through this Invasive Firefox, which logged every site I visited, all the advertising tracking servers that were watching my surfing and all the data they obtained. Then I uploaded the data to my colleagues at The Times, who reconstructed my web sessions into the gloriously invasive picture of my digital life you see here. (The project brought us all very close; among other things, they could see my physical location and my passwords, which I've since changed.)

What did we find? The big story is as you'd expect: that everything you do online is logged in obscene detail, that you have no privacy. And yet, even expecting this, I was bowled over by the scale and detail of the tracking; even for short stints on the web, when I logged into Invasive Firefox just to check facts and catch up on the news, the amount of information collected about my endeavors was staggering.

The session documented here took place on a weekday in June. At the time, I was writing a column about Elizabeth Warren's policy-heavy political strategy, which involved a lot of Google searches, a lot of YouTube videos, and lots of visits to news sites and sites of the candidates themselves. As soon as I logged on that day, I was swarmed — ad trackers surrounded me, and, identifying me by a 19-digit number I think of as a prisoner tag, they followed me from page to page as I traipsed across the web.

Looking at this picture of just a few hours online, what stands out to me now is how ordinary a scene it depicts: I didn't have to visit any shady sites or make any untoward searches — I just had to venture somewhere, anywhere, and I was watched. This is happening every day, all the time, and the only reason we're O.K. with it is that it's happening behind the scenes, in the comfortable shadows. If we all had pictures like this, we might revolt.

Where I live

This tracker for Advertising.com received my almost exact location as latitude and longitude — about a quarter mile off from my actual location. Several other trackers gathered information about where I was, including my city, state, country and zip code. They base this off my IP address, so I had no chance to opt-out. They use the data to conduct targeted advertising but can also use it to track where I'm moving and build a more detailed picture of my interests and activities.

Widgets or trackers?

Tracking scripts like this one for Twitter allow websites to add useful features like share buttons. But the scripts often double as trackers meant to record site visits and build profiles about users. In this case, Twitter can use the information about this page to suggest new followers or sell more targeted advertising on its platform.

My unique identifier: 5535203407606041218

The internet wasn't built to track people across websites. But that didn't stop advertisers. They developed technology to share identifiers among websites. This line connects all trackers that were sharing one of my unique IDs, created by the advertising company AppNexus as I browsed the internet and then stored on my browser for others to use.

Read the rest here:

https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html

Membership Corner

Membership Update

First, I would like to welcome our new members on behalf of the Chapter! When you're participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don't forget to identify yourself as a new member and feel free to ask for help or information. Thanks for joining the Chapter and don't forget to look for opportunities to lend your expertise to improve the Chapter. We're always open to new ideas and suggestions.

New Members August
Brett Larsen
Ryan Dozier
William Droge
Jose Martinez
Joshua Crenshaw
Jeff Baca
Mark Prys
Andrew Funk
Mike Lopez
Tony Capistrano
Rosilio Roman
Jerry Chappee
Rodney Tiner
Daniel Wayland
Marcelle Licciardi
Jeff Dillard
Dae Kwak
Nathan Vogel
Gene Dollarhide

By the time you read this, the Peak Cyber Symposium will be ongoing or completed. It's happening 3—5 September at the DoubleTree by Hilton, Colorado Springs. The Peak Cyber Symposium is also one of our most effective membership recruiting tools that we have. As our membership is holding steady at ~447 members as of the end of August, it is critical that we leverage the Symposium to show potential members the benefits of membership.

Please watch the Newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. As always, if you have any membership questions don't hesitate to contact me.

Thanks,

David Reed

Membership Committee Chairman

membership@issa-cos.org

Cancer research organizations are now the focus of Chinese hacking groups

By Charlie Osborne, ZD Net, August 21, 2019

Chinese advanced persistent threat (APT) groups are honing in on cancer research institutes in recent cyberattacks in order to steal their work, researchers say.

Cancer is the second leading cause of death worldwide and claimed the lives of 9.6 million individuals in 2018. The World Health Organization (WHO) estimates that one in six deaths annually are caused by cancer, and with these high mortality rates, researchers across the globe are working towards ways to improve detection and treatment.

China, too, is contributing -- but cybersecurity firm FireEye says that facing cancer's impact on society, death rates, and the cost of care, the country is not above using nefarious methods to speed up research goals.

On Wednesday, FireEye published a new report on the state of cybercrime in the healthcare industry. Titled, "Beyond Compliance: Cyber Threats and Healthcare," the research claims that Chinese APTs -- many of which are state-sponsored -- continue to target medical entities, and cancer-related organizations are a common target.

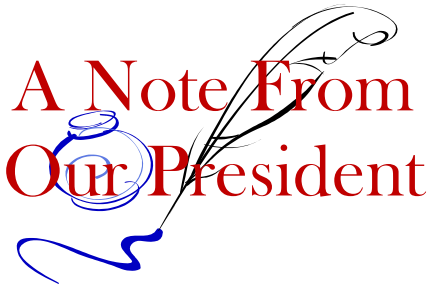
Read the rest here:

https://www.zdnet.com/article/cancer-research-organizations-become-the-new-focus-of-chinese-hacking-groups/

(Continued from page 1)

Two significant events taking place right now in our chapter are the **2019 General Member Survey** and the **2019 Annual Elections**. Here is a little information for both events.

2019 General Member Survey



The purpose of the general members survey is to gain insight from our members on the following topics:

- Registration Fees
- Catering Fees
- Monthly Chapter Meetings
- Annual Award Ceremony

Collectively, the questions represented in these four areas will help our Board of Directors (BoD) shape the planning and programming of our chapter for 2020. Ultimately, we hope to introduce more events that serve to provide new **networking opportunities** for our members that also qualify for **additional CPEs** throughout the year. Please spend **5-minutes** completing this **10-question** survey and help shape the future of our organization. The survey will remain open until September 20th and can be found at: https://www.surveymonkey.com/r/VK2KJN7.

2019 Annual Elections

In September, the BoD will release a "***Call for Candidates***" to help fill specific board positions up for election. Candidates will have time in October to introduce themselves to our general members and publish a candidate article in the October newsletter. Elections will be held in November with results being ratified by the BoD in time for newly elected board members to participate in the December Board Meeting. This year, the following board positions are up for election:

- Executive Vice President
- Chapter Vice President
- Director of Communications
- Vice President of Membership
- Treasure
- Member-at-Large (x2)

Looking further ahead, our October and November chapter lunch meetings will move from HP Enterprise (HPE) to the National Cybersecurity Center (NCC). The HPE facility is scheduled to undergo an extensive remodel which will make the facility inaccessible to our chapter. Coincidently, the NCC recently complete the second phase of their facility build out and is welcoming us with open arms. The newly expanded conference room space at NCC is more than sufficient for our needs and again is being provided to our chapter at no cost. **THANK YOU NCC!!**

In closing, I once again thank all of you for making ISSA-COS the **BEST** chapter globally! Throughout this year, our chapter has received numerous invitations to partner with other organization throughout Colorado Springs. As a result, 2020 is shaping up to be a **stellar year** and I look forward to having all of you along for the ride. On behalf of our BoD, I wish you all a great month.

Sincerely,

Ernest

Our Chapter has a new logo!
Check it out!

ISSA
Information Systems Security Association
Colorado Springs Chapter

Q2 2019 Top-Clicked Phishing Email Subjects from KnowBe4

By Stu Sjouwerman, KnowBe4, July 23, 2019

KnowBe4 reports on the top-clicked phishing emails by subject lines each quarter in three different categories: subjects related to social media, general subjects, and 'In the Wild' - we get those results from the millions of users that click on our Phish Alert Button to report real phishing emails and allow our team to analyze the results.

LinkedIn Continues To Fool Users

Last quarter, more than half of all social media-related phishing emails imitated LinkedIn messages. This trend has been increasing quarter over quarter, likely because there is a perception that they would be legitimate coming from a professional network. It's a significant problem because many LinkedIn users have their accounts tied to their corporate email addresses.

Such a high percentage increases corporate risk of a phishing attack, ransomware breach or other social engineering-related threat. Social media sites in general are being used by cybercriminals as phish bait more and more each quarter. According to recent research from Vade Secure, social media phishing attacks are up by more than 70%.

“It feels good to ‘join my network’ or connect with someone in some way – that’s why social media phishing attacks are so successful,” said Stu Sjouwerman, CEO of KnowBe4. “Users innately trust their ‘verified’ contacts so are more apt to click on a link that come from someone they know. It’s becoming harder to identify phishing attacks, but our users are smarter than the bad guys think and can absolutely be trained to identify and avoid phishing and social engineering attacks."

Read the rest and view an excellent infographic here:

https://blog.knowbe4.com/q2-2019-top-clicked-phishing-email-subjects-from-knowbe4-infographic

Why You Should Never Borrow Someone Else's Charging Cable

By Suzanne Rowan Kelleher, Forbes, August 15, 2019

We've all been there. Your smartphone or tablet is low on power and you've left your charging cable at home. There's no harm in borrowing one from a fellow passenger in the airport departure lounge or from your hotel's front desk clerk, right?

In 2019, that would be a huge mistake, say cybersecurity experts.

“There are certain things in life that you just don't borrow,” says Charles Henderson, Global Managing Partner and Head of X-Force Red at IBM Security. “If you were on a trip and realized you forgot to pack underwear, you wouldn't ask all your co-travelers if you could borrow their underwear. You'd go to a store and buy new underwear.”

Henderson runs a team of hackers that clients hire to break into their computer systems in order to expose vulnerabilities. Since cyberhackers have figured out how to implant charging cables with malware that can remotely hijack devices and computers, his team sometimes uses a trick to teach clients to be less trusting of third-party charging cables. “We might send somebody a swag iPhone cable in the mail. Maybe we have it branded as something innocuous, like a vendor or a partner that they have listed on their website. We send off the cable and see if the person plugs it in,” he says.

Last week, at the annual DEF CON Hacking Conference in Las Vegas — “hacker summer camp,” says Henderson — a hacker who goes by "MG” demonstrated an iPhone lightning cable that he had modified. After using the cable to connect an iPod to a Mac computer, MG remotely accessed the cable's IP address and took control of the Mac, as Vice reported in play-by-play fashion. MG noted that he could later remotely “kill” the implanted malware and wipe out all evidence of its existence. The enterprising hacker had a stash of so-called O.MG cables that he was selling for $200 apiece.

Malicious charging cables aren't a widespread threat at this time, says Henderson, “Mainly because this kind of attack doesn't scale real well, so if you saw it, it would be a very targeted attack.”

“But just because we haven't yet seen a widespread attack doesn't mean we won't see it, because it certainly does work,” says Henderson. “The technology is really small and really cheap. It can get so small that it looks like an ordinary cable but has the capability and the intelligence to plant malware on its victim. These things are only going to get cheaper to produce and it's not something your average consumer is going to be tracking to know when it becomes viable on a mass scale.”

For the moment, Henderson says, a bigger threat than malicious charging cables is USB charging stations you see in public places like airports. “We've seen a couple of instances where people modified charging stations. I'm not talking about an electrical outlet, I'm talking about when there's a USB port on a charging station.”

Read the rest here:

https://www.forbes.com/sites/suzannerowankelleher/2019/08/15/why-you-should-never-borrow-someone-elses-charging-cable/#201158a039a3

IoT and Network Security

By April Frost , ISSA-COS, August 15, 2019

We love being connected: Before I get out of bed in the morning, I can check my security system, work and home email, all social media, and ask Alexa what the weather will be. I can let my cat outside and track her journey via her GPS collar, which is connected to my smartphone. In my car, I use my Waze app to find the best way to work, including speed traps and necessary detours. Before I get to work, I use my phone to tell my first-generation iKettle to boil water for my tea; I receive a notification when the water is ready, and the iKettle keeps the water hot until I am ready to drink it. I log into my work computer, tell Alexa to remind me of my day, and check in on my cat. I video chat with my co-worker to schedule lunch, and my day is off to a great start.

My network manager stops by my office to tell me that the company is reducing the IoT footprint in our company. I must get rid of my iKettle, Alexa, and keep my smartphone turned off, or not connected to the company's wi-fi. I can keep my watch on, but I must turn off Bluetooth until I leave work. This guy is crazy; how will I get my work done, make sure I get all my steps in, answer my personal phone calls, and check on my cat? [1]

What is the IoT

The Internet of Things (IoT) is literally everything that is connected to the internet without human interaction. Common items, like laptops, PCs, printers, and now smartphones, are not considered IoT devices since they are configured before connecting. I could not begin to list every item, but some are: lightbulbs, thermostats, voice command devices, sensors that monitor the environment, wearable devices, microchips, tea kettles, and wearable devices, including even Levi's Commuter X Jacquard by Google smart jacket. IoT devices are generally easy to hack because they are not designed to be upgraded or patched; they are essentially devices that connect to the internet with minimal configuration.

The IIoT is the Industrial Internet of Things, also known as Industry 4.0. The IIoT is the business version of IoT, which includes environmental data sensors, thermostats, meters, wireless networks, and other tools used to analyze and measure industrial processes. (In this article, IoT will refer to all IoT and IIoT devices.)

It is expected that there will be up to 40 *billion* IoT devices in use by 2020. More than half will be consumer devices, such as smart TVs and voice-activated speakers. Many of those consumer devices will also end up in the workplace. How do we manage devices that do not require human interaction on company networks? Several recent surveys indicated that less than 20% of all businesses would be able to identify all the IoT devices on their network.

What network vulnerabilities are associated with IoT

Vulnerability: the state of being exposed to the possibility of being attacked or harmed.

When the iKettle was created, the password was hard-coded into the system. It was easy to hack, and once the iKettle was hacked, the attacker could gain access into the user's home wi-fi. (The second- and third- generation models are more secure. The iKettle has never been sold in the US, but there are similar devices available.) [2]

Having personal devices like the iKettle at work, shows the IoT footprint per user is far greater than just one device per person. Each person may have a wearable device or two (besides step counters, don't forget heart monitors and glucose pumps), smart speakers, and the list goes on. Connecting more and more IoT devices to networks increases the risk of hackers discovering and attacking the network through these devices. Specifically, an IIoT network hack could lead to industrial espionage or even critical infrastructure damage.

Today I discovered this article (released on August 13, 2019), which described the Alexa at SLU initiative at St Louis University. [3] St Louis University (SLU) is in its second year of providing the Amazon Echo Dot in every dorm room on campus. The 2,300 second-generation Echo Dots are powered by Amazon's Alexa for Business platform using a private SLU skill, so the Echo Dots are limited in what information they can provide. They are not linked to any student information, including their Amazon Prime account(s). There is a sticker on each device with the MAC address and the dorm room number, but no data is gathered about the room, the people asking questions, or even the questions being asked. Students can get answers to about 135 questions from the Echo Dot, such as the weather, hours the library is open, and general information. Students can only stream music through the university's iHeartRadio subscription. Calls can be made to anyone in the university's directory of contacts, including local businesses, such as the nearby sandwich shop, which is open until 3:30am. The school is considering making the SLU skill public, so students who live off campus can also access the SLU-related information.

The reason the IoT is getting so much attention is that every IoT device on a network expands the attack surface. IoT devices were not originally considered threats, but when they are attached to a network, they become another access point for a network security breach. Instead of the network only being exposed by the number of computers/users connected, today's exposure includes: multiple personal devices, thermostats, all sensors (motion, temperature, security, etc.), phone systems, door monitoring, and the list goes on.

Many IoT devices were not designed with security in mind. In large companies, the facilities and operations managers did

(Continued on page 7)

(Continued from page 6)

not communicate with IT on a regular basis. "This creates islands of self-contained information. The problem is, should one system/group see an issue, it is only seen on their system. *This lack of interconnected view is what hackers exploit,*" said Colin Tankard, managing director of Digital Pathways. [4] It is easy to add or upgrade an existing device (postage meter, HVAC control), and not realize that the device is now an attack surface on the network. The involvement of IT in every part of company operations is now imperative.

Examples of IoT Attacks and Exposures [5]

Here are some random examples of network attacks and exposures due to IoT devices and unsecured networks.

1. A casino fish tank was connected to the internet to automatically feed the fish and regulate their environment was hacked. Hackers gained access to the casino network through the smart thermometer in the aquarium and copied a database of high-roller information out of the network to a site in Finland. Darktrace, a cyber defense company involved in this case, reported this attack.
2. State-sponsored Russian hackers are targeting IoT devices to breach enterprise networks, according to the Microsoft Threat Intelligence Center. In April 2019, hackers were spotted attempting to exploit a VoIP phone, printer, and video decoder at multiple locations. In two cases, the default passwords on the devices had never been changed, and the third device had not been patched with the latest security update. [6]
3. Not exactly a network-based exploit, but we all drive: Hackers took remote control over a Jeep driving down the highway. The hackers took over a Wired reporter's 2014 Jeep entertainment system, taking over the fan, radio, steering, transmission, and brakes, by exploiting the car's internet-connected control platform, UConnect. This platform is available on most late-model Chrysler vehicles.
4. Here's a classic, unexpected IoT vulnerability: A white LIFX Mini light bulb saves the wi-fi password in plaintext on the bulb during initial setup. Anyone who steals the bulb from a light fixture at your home or finds one in the trash can get right into your home network.
5. Delta Controls industrial control system vulnerability: (Delta Controls is one of the most respected organizations in the industry) McAfee Security exposed a flaw in which hackers can take over control systems such as temperature controls, cause power surges to a building or grid, or alter alarms, all of which could disable or destroy critical data and equipment. The vulnerability is nothing more than a buffer overflow error, in which the system attempts to write more data than the memory block can accept. McAfee Security called this vulnerability a twisted version of Marco Polo, in which the hacker shouts 'Marco' and waits for the system to respond with 'Polo'. A beta version of a security patch is already available. [7]

Solutions and Risk Mitigation

There is not one easy solution, or combination of solutions to insure any network (or device) will not be hacked. Keeping a small network footprint, perform regular penetration tests, using encryption, and patching all devices are great practices to apply.

To reduce exposure, companies must secure their networks by isolating all critical components and using data encryption in network connections. The current state of IoT technology makes that difficult, as does the lack of consistency in security planning for IoT devices and technologies. Without regular scans of the network, IT managers will not know what devices are on their networks at any time. Company-wide policies can raise awareness for all employees, and these policies must be supported by upper management to aid in enforcement.

Most IoT devices only need to be connected to the internet initially to configure themselves to the environment. The communication to these devices after configuration can be limited to one channel between the device and the remote server. Fewer communication paths between devices reduces the network's attack surface.

Where possible, it is helpful to isolate or segment the network to reduce the attack surface into small sections. This can be done with switch and vlan configurations, as well as Access Control Lists (ACLs). The same security policies must be applied to all sections of the network consistently. Management should be done with network access control (NAC) software, Intrusion Detection/Intrusion Protection Systems (IDS/IPS), and system alerts.

In June of 2019, the National Institute of Standards and Technology (NIST) released the first in a series of documents to help IoT device users protect themselves, their data, and their networks in an enterprise setting. The 44-page document, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228) is considered a companion to the NIST Cybersecurity Framework and SP 800-53 Rev.5 resources. These documents are aimed at larger corporations, who have more to lose in a cybersecurity attack, but provide helpful guidelines for any size business. NISTIR 8228 only offers suggestions; none of the contents are FISMA (Federal Information Security Management Act) requirements. More documents in this series are expected soon.

The Executive Summary of NISTIR 8228 defines three considerations and mitigation goals specifically for IoT device management compared to conventional IT devices, regarding cybersecurity and privacy risks: [8]

1. IoT devices interact with the physical world in ways conventional IT devices do not. Operational requirements for IoT devices may need to be specifically addressed.

(Continued on page 8)

(Continued from page 7)

2. IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can. It may be necessary to manually manage large quantities of IoT devices, which requires additional staff and tools, as well as addressing risks associated with third-party vendors and possible remote access.
3. The availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional IT devices. Organizations may have to select, implement, and manage additional controls, as well as determine how to respond to risk when adequate controls for mitigating risk are not available.

The mitigation goals suggested by NISTIR 8228 authors are aimed at IoT devices and the privacy risks associated with them, as compared to conventional IT devices:

1. Protect device security – prevent IoT devices from being used to conduct attacks
2. Protect security of data – secure personally identifiable information
3. Protect individuals' privacy – minimize personal exposure

These guidelines raise awareness to the security risks associated with IoT technology and help users face these challenges head-on.

California's SB-327 is the country's first IoT security law. It passed September 28, 2018, effective January 1, 2020. The bill requires companies who manufacture connected devices "to equip (each) device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified." [9] The bill applies to manufacturers of connected devices that are sold or offered or sale in California. Any HIPAA-related entity or device is excluded from this bill. Points that are vaguely covered include software updates or patches. Any third-party software or apps that a user adds to the device are excluded, which means the bill covers devices sold in California, nothing else about the device or its use.

There was a bill introduced in the Senate in March of this year, S.734 – Cybersecurity Improvement Act of 2019, to encourage increased cybersecurity for IoT devices, but as of June 19, it is still stuck in the Senate. House bill, H.R.6032 - SMART IoT Act, passed November 2, 2018, which directs the Department of Commerce to conduct a study of the IoT industry in the US. These bills still are about discovery, instead of mandating security actions at any level.

As an IT manager, the best plan of attack to keep your company safe, is to follow the guidelines provided by the Open Web Application Security Project (OWASP) Internet of Things Project. OWASP provides extensive, free resources for all things internet-related. The IoT Project includes Principles of IoT Security, as well as a Top 10 List of things to avoid. The Principles of IoT Security include topics such as controlling the edge of the network, hardening the system, managing the lifecycle of all devices, planning for the worst, and mostly understanding that mistakes happen. If you assume that your network is secure and un-hackable, you are already more vulnerable, because attacks happen every day, even to the most careful IT managers. Constant vigilance of a company network includes so many items: regular automated device ID and discovery, frequent penetration testing, encrypting data at rest and in motion, monitoring for abnormal behavior, and enforced policies on things such as passwords and workspace security. Determining what devices (of any type) are allowed on the network is a good place to start with upper management's buy-in. From that point, denying any anonymous connections and using the network to enforce these rules will aid you in managing a secure network.

The End...or Just the Beginning

This is a brief introduction to associate the connection between network security and the ever-changing world of IoT devices. There is no one specific way to keep a company network safe and secure, except to keep learning, testing, and patching all devices that are connected.

END NOTES

[1] Disclaimers: I do not have Alexa, an iKettle, or a cat. I also do not drink tea. All are referenced as hypothetical examples.

[2] Ng, A. (2017). *How your home Wi-Fi security could end up in hot water*. [online] CNET. Available at: https://www.cnet.com/news/smart-tea-kettle-home-wi-fi-security-hot-water/ [Accessed 12 Aug. 2019].

[3] Price, M. (2019). *Alexa, time for class: How one university put an Echo Dot in every dorm room*. [online] CNET. Available at: https://www.cnet.com/features/alexa-time-for-class-how-one-university-put-an-echo-dot-in-every-dorm-room/?ftag=CAD1acfa04&bhid=*233265216662521646356196634424 62 [Accessed 13 Aug. 2019].*

[4] Allison, P. (2019). *Network security in the age of the internet of things*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/feature/Network-security-in-the-age-of-the-internet-of-things?src=5759962&asrc=EM_ERU_96809218&utm_content=eru-rd2-rcpB&utm_medium=EM&utm_source=ERU&utm_campaign=20180626_ERU%20Transmission%20for%2006/26/2018%20(UserUniverse:%202604989) [Accessed 10 Aug. 2019].

(Continued on page 9)

(Continued from page 8)

[5] All examples except numbers 2 and 5 are from the article: King, B. (2019). *7 Scary Internet of Things Hacks and Exploits That Really Happened*. [online] MakeUseOf. Available at: https://www.makeuseof.com/tag/internet-of-things-hacks-exploits/ [Accessed 13 Aug. 2019].

[6] Cimpanu, C. (2019). *Microsoft: Russian state hackers are using IoT devices to breach enterprise networks | ZDNet*. [online] ZDNet. Available at: https://www.zdnet.com/article/microsoft-russian-state-hackers-are-using-iot-devices-to-breach-enterprise-networks/ [Accessed 13 Aug. 2019].

[7] Ashford, W. (2019). *McAfee warns of serious security flaw in building controller*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/news/252468156/McAfee-warns-of-serious-security-flaw-in-building-controller [Accessed 13 Aug. 2019].

[8] Boeckl, K., Fagan, M. et.al. (2019). [online] Nvlpubs.nist.gov. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf [Accessed 12 Aug. 2019].

[9] California Senate (2018). *SB-327*. Sacramento, pp.1-2.

Breakfast with ISSA-COS

ISSA-COS will arrange for Oliver's Deli to come sell breakfast at your office!

Patrons will receive a **15% discount** on all food items…*compliments of ISSA-COS!*

An ISSA-COS representative will be on hand to provide membership and sponsorship information.

Nominate your company and

YOU EAT FREE!

Volunteer Opportunities

Board Positions	Key Personnel	Volunteer Corps
Deputy Recorder/Historian	**SIG Committee Chair**	**Increase community awareness of our chapter**
Deputy Treasurer	**Recognition Committee Chair**	**Expand community involvement for our members**
Deputy VP of Training	**SIG Leaders:**	**Attend industry relevant events throughout Colorado**
Member-at-Large	• ***Finance***	**Earn additional CPE/CPU credits**
	• ***Retail***	**Increase network**
	• ***Educators***	
	• ***Executives***	

Platinum Sponsor—Murray Security Services—
https://www.murraysecurityservices.com/

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Aero Sponsor—CT Cubed
https://www.ctcubed.com/

Update Your Profile!

Don't forget to periodically logon to *www.issa.org* and update your personal information.

A Major Cyber Attack Could Be Just as Deadly as Nuclear Weapons, Says Scientist

By Jeremy Straub, Science Alert, August 18, 2019

People around the world may be worried about nuclear tensions rising, but I think they're missing the fact that a major cyberattack could be just as damaging – and hackers are already laying the groundwork.

With the US and Russia pulling out of a key nuclear weapons pact – and beginning to develop new nuclear weapons – plus Iran tensions and North Korea again test-launching missiles, the global threat to civilization is high. Some fear a new nuclear arms race.

That threat is serious – but another could be as serious, and is less visible to the public. So far, most of the well-known hacking incidents, even those with foreign government backing, have done little more than steal data.

Unfortunately, there are signs that hackers have placed malicious software inside US power and water systems, where it's lying in wait, ready to be triggered. The US military has also reportedly penetrated the computers that control Russian electrical systems.

Many intrusions already

As someone who studies cybersecurity and information warfare, I'm concerned that a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon.

Unlike a nuclear weapon, which would vaporize people within 100 feet and kill almost everyone within a half-mile, the death toll from most cyberattacks would be slower. People might die from a lack of food, power or gas for heator from car crashes resulting from a corrupted traffic light system. This could happen over a wide area, resulting in mass injury and even deaths.

This might sound alarmist, but look at what has been happening in recent years, in the US and around the world.

In early 2016, hackers took control of a US treatment plant for drinking water, and changed the chemical mixture used to purify the water. If changes had been made – and gone unnoticed – this could have led to poisonings, an unusable water supply and a lack of water.

In 2016 and 2017, hackers shut down major sections of the power grid in Ukraine. This attack was milder than it could have been, as no equipment was destroyed during it, despite the ability to do so. Officials think it was designed to send a message.

In 2018, unknown cybercriminals gained access throughout the United Kingdom's electricity system; in 2019 a similar incursion may have penetrated the US grid.

In August 2017, a Saudi Arabian petrochemical plant was hit by hackers who tried to blow up equipment by taking control of the same types of electronics used in industrial facilities of all kinds throughout the world.

Just a few months later, hackers shut down monitoring systems for oil and gas pipelines across the US This primarily caused logistical problems – but it showed how an insecure contractor's systems could potentially cause problems for primary ones.

The FBI has even warned that hackers are targeting nuclear facilities. A compromised nuclear facility could result in the discharge of radioactive material, chemicals or even possibly a reactor meltdown.

A cyberattack could cause an event similar to the incident in Chernobyl. That explosion, caused by inadvertent error, resulted in 50 deaths and evacuation of 120,000 and has left parts of the region uninhabitable for thousands of years into the future.

Mutual assured destruction

My concern is not intended to downplay the devastating and immediate effects of a nuclear attack. Rather, it's to point out that some of the international protections against nuclear conflicts don't exist for cyberattacks.

For instance, the idea of "mutual assured destruction" suggests that no country should launch a nuclear weapon at another nuclear-armed nation: The launch would likely be detected, and the target nation would launch its own weapons in response, destroying both nations.

Read the rest here:

https://www.sciencealert.com/a-major-cyber-attack-could-be-just-as-damaging-as-a-nuclear-weapon

2019 Schedule of Events

Chapter Meetings – Dinner

Tuesday, October 15, 2019

Tuesday, November 19, 2019

Chapter Meetings – Lunch

Wednesday, October 16, 2019

Wednesday, November 20, 2019

Board Meeting

TBD

Mini-Seminars

Saturday, October 19, 2019

Saturday, November 23, 2019

Special Interest Group Gatherings (see Page 13)

Thursday, September 5, 2019

Thursday, December 5, 2019

ISSA-COS Conferences
Peak Cyber

Tuesday, September 3, 2019

Wednesday, September 4, 2019

Thursday, September 5, 2019

Quarterly Recognition & Networking Events

Tuesday, September 3, 2019

Thursday, December 5, 2019

Security +CE Reviews

Saturday, September 14, 2019

Saturday, September 21, 2019

Saturday, September 28, 2019

Annual Award Ceremony

Thursday, December 5, 2019

For additional information, contact info@issa-cos.org or visit www.issa-cos.org.

From the Mentorship Team

ISSA-COS Mentorship is available as an embedded feature/service which is matrixed through each SIG. This custom-tailors ISSA-COS Mentorship so that it tailor-fits each career lifecycle stage and special interest. ISSA Mentors and Proteges aren't enrolled into a mentorship program; rather, the process is that of an intake in which a need is assessed with the goal of the need being met. The need is taken in and evaluated and an action plan is created to meet the need. (As an additional need arises, an additional intake is created.)

ISSA Mentorship is an exchange in which both parties are protected and respected. Healthy boundaries are maintained and proprietary knowledge is protected. ISSA Mentorship is designed to be a win-win situation in which both parties are enriched.

ISSA Mentorship is goal/need-driven. The ISSA-COS Mentorship Intake Form serves as a guide regarding the length of the mentorship session as the goal/need of the mentor or protege will determine parameters. The carefully-crafted intake form provides ISSA-COS leadership with metrics so that ISSA Mentorship is treated as a service with KPIs (Key Performance Indicators) and next step suggestions. If ISSA-COS Mentorship can *measurably* boost the careers of its membership, ISSA will, in turn, be boosted as we become known for building each other.

Mentorship Intake Form

email completed form to: mentorship@issa-cos.org

Colorado Springs Chapter
ISSA
Information Systems Security Association

I seek to:

- ❑ mentor
- ❑ protégé
- ❑ peer-to-peer

I aim to meet:

- ❑ in person
- ❑ by phone
- ❑ via email
- ❑ via Skype

What drives you to invest in mentorship now? Please state two goals:_____

_____

_____

_____

_____

_____

Name:_____

Phone:_____

Email:

_____

_____

Checkmark your current status in the ISSA Cyber Security Career Lifecycle:

Are you on LinkedIn? Y / N
Are you on Skype? Y / N

Have you visited the ISSA-COS website? Y / N

Which ISSA committees or special interest groups align with your interests?

- ❑ Speakers Bureau
- ❑ Friends of Authors
- ❑ Women in Security
- ❑ Healthcare in Security
- ❑ Finance in Security
- ❑ Retail in Security
- ❑ DoD in Security
- ❑ Executives in Security
- ❑ Young Professionals in Security
- ❑ certification prep
- ❑ continuing education
- ❑ other: _____

My mentorship goals align most closely with:

- ❑ career advice
- ❑ building an alliance
- ❑ seeking opportunity
- ❑ technical training
- ❑ practice leadership
- ❑ practice speaking
- ❑ practice authoring for publications
- ❑ solving a specific technical challenge
- ❑ finding my place in our ISSA chapter
- ❑ other _____

MENTOR USE ONLY

Feedback / Recommendations

Time invested:____ mins / hrs

Were goals met? Y / N

Is additional mentorship requested at this time? Y / N

Additional notes:

OFFICE USE ONLY

Follow-up Plan

- ❑ *time recorded*
- ❑ *goals recorded*
- ❑ *resources provided*
- ❑ *referred to SIG:* _____

Next steps:

IBM researchers show how "warshipping" turns physical mail into a hacking vector

By Maria Deutcher, Silicon Angle, August 7, 2019

CEOs and other senior board-level executives are exposing their organisations to cyberattacks and hackers because of a lack of awareness around cybersecurity, a new study has warned.

As if ransomware and state-sponsored hacking campaigns didn't give enterprises enough cause for concern, there's now yet another cybersecurity threat to reckon with: "warshipping."

That's the name IBM Corp.'s X-Force Red group has given to a creative hacking method it detailed today. The group helps IBM's enterprise customers probe their networks for security weaknesses and also researches new methods that cyber criminals may use to carry out attacks.

When a hacker doesn't find a weakness in a network, warshipping can allow them to create one. The basic idea is to build a remote-controlled device capable of launching a cyberattack and physically mail it to the victim. The technique exploits the fact that companies don't always thoroughly check the packages passing through their mailrooms, especially when they come in an innocuous-looking box bearing the logo of a supplier or popular e-commerce site.

Warshipping has already been successfully tested in the field. In a blog post, X-Force Red head Charles Henderson wrote that his team used the technique to defeat the defenses of several corporate networks as part of penetration testing work done for customers.

The researchers pulled it off with a simple hand-built computer they cobbled together from off-the-shelf components. The device, which cost about $100 to assemble, consisted of a single circuit board packing a 3G modem for communicating with a remote-control server and executing attacks.

"While in transit, the device does periodic basic wireless scans, similar to what a laptop does when looking for Wi-Fi hotspots. It transmits its location coordinates via GPS back to the C&C [command and control server," Henderson detailed.

"Once we see that a warship device has arrived at the target's front door, mailroom or loading dock, we are able to remotely control the system and run tools to either passively or actively attempt to attack the target's wireless access," he elaborated. "The goal of these attacks is to obtain data that can be cracked by more powerful systems in the lab."

One way a warshipping device can facilitate cyberattacks is by intercepting the initial packets that an employee device such a phone sends to a company's network when it establishes a wireless connection. This data is usually encrypted but can theoretically be unscrambled to obtain the Wi-Fi password. A warshipping device can also deploy a decoy Wi-Fi network to fool users into entering their login credentials.

Read the rest here:

https://siliconangle.com/2019/08/07/ibm-researchers-warshipping-hacking-tool/

Ransomware Attack Hits Local Governments In Texas

By Trey Shaar, KUT, August16, 2019

A coordinated ransomware attack has affected at least 20 local government entities in Texas, the Texas Department of Information Resources said. It would not release information about which local governments have been affected.

The department said the Texas Division of Emergency Management is coordinating support from other state agencies through the Texas State Operations Center at DPS headquarters in Austin.

DIR said the Texas Military Department and the Texas A&M University Systems' Cyber-Response and Security Operations Center teams are deploying resources to "the most critically impacted jurisdictions."

Elliot Sprehe, press secretary for the department, said DIR was working to confirm which government entities are affected and said other information was still coming in.

"It looks like we found out earlier today, but we're not currently releasing who's impacted due to security concerns," he said.

Read the rest here:

https://www.kut.org/post/ransomware-attack-hits-local-governments-texas

SPECIAL INTEREST GROUPS (SIGS)

Special Interest Groups (SIGs) are groups comprised of Cybersecurity professionals who gather together to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: Affinity Groups and Industry Groups. On a quarterly basis, ISSA-COS brings together both groups to participate in formally structured events. During these gatherings, participants have an opportunity to first attend one of four (4) Affinity Groups then, one of four (4) Industry Groups. CPEs/CPUs are awarded for attend these events.

In-between formal gatherings, the SIG Leaders for each individual SIG are encouraged to coordinate informal gatherings. ISSA-COS encourages SIG leaders to consider hosting informal gatherings at social venues such as sporting events, restaurants, bars, or breweries. Informal gatherings may also include participating in a community improvement project, a group walk or hike, or a picnic/BBQ.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups gather to share security related experiences, impart knowledge and education, and help one another solve common problems and issues. The Affinity Groups currently promoted by ISSA-COS include:

Women in Security – **W***[omen]***IS**

Young Professional in Security – **Y***[oung Professionals]***IS**

Mentoring in Security – **M***[entoring]***IS**

Executives in Security – **E***[xecutives]***IS**

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups gather together to discuss security related topics and share solutions to problems affecting their perspective industries. They also exchange Cybersecurity related tips, information, and education specific to their industries. The Industry Groups currently promoted by ISSA-COS include:

Finance in Security – **F***[inance]***IS**

Healthcare in Security – **H***[ealthcare]***IS**

Retail in Security – **R***[etail]***IS**

DoD in Security – **D***[oD]***IS**

ISSA-COS invites you to join us at our next SIG gathering or any one of our many other events.

For additional information, contact: info@issa-cos.org or visit www.issa-cos.org.

AEMO 'concerned' about nation-state attacks on power grids

By Stilgherrian, ZD Net, August 22, 2019

"For the energy sectors and critical infrastructure sectors, particularly around electricity, we are concerned about nation-state actors," says Tim Daly, chief security officer (CSO) for the Australian Energy Market Operator (AEMO).

"Nation-states are looking to have capability and implants that are persistent within critical organisations," he told the Gartner Security and Risk Management Summit in Sydney on Tuesday.

"We are concerned about Australia being targeted by that kind of activity," he said, because ransomware and other attacks are increasingly being targeted at specific industry verticals.

In the US, municipal governments have been targeted, and the energy sector could be next.

AEMO is working to make sure individual organisations are improving their cyber resilience, as well as considering how they would respond to a coordinated attack against the energy sector.

Supply chain security is definitely a concern, Daly said. Potential problems range from attacks on suppliers such as in the PageUp data breach, to the CloudHopper campaign against managed service providers.

Another challenge is the changing nature of the electricity grid, with the introduction of distributed energy resources such as rooftop solar.

"That's millions of devices, potentially Internet of Things, internet connected, all different kinds of vendors, so that's a fairly wicked supply chain issue that we need to lean into," Daly said.

"It's going to be a challenge over the coming years."

IT'S ABOUT PEOPLE AND CULTURE CHANGE, AS ALWAYS

In Western Australia, Horizon Power is already working on improving cyber resilience in its distributed energy resources.

They've been tackling some of the cultural issues while developing their Distributed Energy Management System (DERMS), which is now part of their core strategy.

Horizon serves more than 49,000 customers spread across 2.3 million square kilometres. It handles all three of the elements -- electricity generation, distribution, and retail -- for 38 separate systems across the state.

Advanced smart meters have also been deployed to its customer base.

"We've moved away from that centralised generation and transmission [model], to very discrete units or microgrids which provided electricity to those areas," said Horizon's chief information security officer (CISO), Jeff Campbell.

"We saw customers embracing this concept of being in charge of their own electricity, potentially feeding into connected grids, that they could manage and trade electricity," he said.

The introduction of smart meters has meant that Horizon now has sensors to monitor outages and other faults at every endpoint, in addition to gaining a way to get the telemetry needed for trading. It has also meant they can offer pay-as-you-go billing.

Knowing each customer's usage patterns has proved useful for managing the system as a whole and for predictive maintenance.

On the customer side, customers might have their own devices -- like air conditioners and swimming pool pumps -- behind their smart meters that could be used to access and trade data in order to help make decisions on energy use.

Read the rest here:

https://www.zdnet.com/article/ameo-concerned-about-nation-state-attacks-on-power-grids/

Texas ransomware attacks deliver wake-up call to cities

By Maggie Miller, The Hill, August 22, 2018

A recent spree of ransomware attacks in Texas has highlighted the increasing threat they pose to city governments, with experts warning the "lucrative" attacks won't go away.

The Texas Department of Information Resources has confirmed that 22 Texas entities, mostly local governments, have been hit by the ransomware attacks that took place late last week. The department pointed to a “single threat actor” as being responsible for the attacks, which did not impact any statewide systems.

While the agency has refused to identify which entities were attacked due to an ongoing investigation, the governments of Keene, Texas and Borger, Texas, announced this week that they were among those impacted, with the attacks making it difficult for the two towns to handle utility payments from residents.

Keene Mayor Gary Heinrich told NPR’s "Morning Edition" on Tuesday that the hackers, who have not been identified, have demanded $2.5 million from the towns and other entities impacted collectively. Heinrich called the attackers “stupid people” for expecting Keene to pay up to regain access to their systems.

For experts, the spate of attacks on small towns is delivering a wake-up call to government officials.

One top expert emphasized that such attacks, which involve a malicious actor encrypting computer systems of an entity or group and demanding payment to return them to normal, are among the most common types of cyberattacks.

“It’s certainly one of the most prevalent, certainly one of the most lucrative, that keeps it in the top five lists of threats that are out there,” Mark Orlando, the chief technology officer of cyber protection solutions at Raytheon Intelligence, Information and Services, told The Hill.

There have been a string of ransomware attacks on other cities around the United States prior to the Texas attacks that appear to back up Orlando.

And the ransomware attacks often force tough choices on their victims.

In May, city systems in Baltimore were taken out by a debilitating cyberattack, with hackers demanding $76,000 to give the city access again to its systems. But Baltimore's mayor refused to pay the ransom, a costly decision for the city. According to the CBS affiliate in Baltimore, as of June, the city had spent $18 million to get city employee email accounts back up and running, along with other fixes.

In 2018, Atlanta was hit by a similar attack, with hackers demanding the equivalent of over $50,000 in bitcoin. Atlanta also chose to spend millions to address the results of the attack rather than pay the ransom.

The Department of Justice (DOJ) later indicted two Iranian men for deploying the SamSam malware virus against Atlanta, the government of Newark, N.J., the Port of San Diego, and hospitals and public institutions around the United States. In total, the DOJ estimated that hackers caused the loss of $300 million for their victims.

Some cities that have been attacked have chosen to pay the ransom instead of spending more to replace computer systems.

In June, the leaders of Riviera Beach, Fla. paid hackers almost $600,000 in bitcoin to gain back access to their computer systems. The attack occurred after a city employee opened an email that contained the ransomware virus.

Orlando said the approach taken by cities in response to ransomware attacks often depends on their size and resources available.

“Baltimore for example, they chose not to pay, and instead spent a lot of money reconstituting their networks, they took the hit,” Orlando said. “It’s hard to ignore the pattern that we’ve had some large cities that were able to find the funds to rebuild, and then we’ve seen the smaller municipalities that choose the other direction.”

Cities are not alone in responding to these ransomware attacks. In Texas, the FBI, the Department of Homeland Security (DHS), and the Federal Emergency Management Agency are among the federal agencies responding to and investigating the ransomware incidents. The FBI also responded to the attack on Baltimore.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) has published guidelines that it recommends organizations follow in regard to protecting themselves against ransomware attacks. Those recommendations include updating software, not clicking links in unsolicited emails, and backing up data on a regular basis.

Read the rest here:

https://thehill.com/policy/cybersecurity/458357-texas-ransomware-attacks-deliver-wake-up-call-to-cities

It's Official: Defense Department Will Use Other Agencies' Cloud Security Assessments

By Aaron Boyd, NextGov, August 16, 2018

The Defense Information Systems Agency announced a provisional authorization Thursday that will speed up cloud deployments by eliminating some of the Defense Department's oversight over security authorizations.

Defense components had been waiting on the rule, which will allow them to purchase and deploy cloud products and services at the moderate security level—impact level two—without having to ask for written permission.

"This authorization allows for data designated publicly releasable or IL2, to be stored in the cloud on authorized FedRAMP offerings without waiting for DOD to issue a specific authorization document," said Roger Greenwell, the risk management executive and authorizing official at DISA. "We worked with officials from the DOD, Chief Information Office and mission partners on the drafting of the policy, and believe this approach provides significant benefit to both the DOD community as well as the cloud industry."

Previously, Defense offices were required to do their own security assessments on systems, issuing a program- or department-level authority to operate, or ATO. But this system worked directly against the promise of the Federal Risk and Authorization Management Program, or FedRAMP, which was designed to facilitate the certification process and allow agencies to reuse the ATO work done at other departments.

The reuse issue—called "reciprocity"—has been a sticking point since FedRAMP was launched in 2011. Since that time, administration officials and lawmakers have pushed agencies to reuse more ATOs whenever appropriate.

"What was supposed to be an expedited process—six months, maybe costing a quarter of a million dollars—instead, in many cases, took years—and takes years—and can cost companies millions of dollars, the very opposite of what FedRAMP was designed to achieve," Rep. Gerry Connolly, D-Va., said during a hearing July 17 held by the House Oversight Subcommittee on Government Operations. "We can't leverage the potential of cloud computing if the processes are slower than the speed at which the technology itself advances."

Jack Wilmer, Defense Department deputy chief information officer for cybersecurity, previewed the pending rule during the hearing.

"We are fully committed to reciprocity. There's a massive incentive for us in having that reciprocal arrangement with FedRAMP," Wilmer said. "Going through those 325 [controls] at the moderate baseline, as an example, which is something that the FedRAMP program takes on for us, is something we no longer have to do in order to leverage those cloud services."

The blanket agreement comes with some caveats, however. The rule only applies to solutions approved at the moderate baseline through FedRAMP and listed in the program's marketplace. Even then, Defense offices can only reuse authorizations from companies whose data centers are physically located in the U.S. or its territories.

The covered products also have to maintain their FedRAMP ATO and agree to continuous monitoring.

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/08/its-official-defense-department-will-use-other-agencies-cloud-security-assessments/159241/

Lack of cybersecurity is the biggest economic threat to the world over the next decade, CEOs say

By Marc Wilzczek, CIO, August 21, 2019

In its 2019 CEO Imperative Study, Ernst & Young surveyed 200 global CEOs from the Forbes Global 2000 and Forbes Largest Private Companies across the Americas, Europe, the Middle East, Africa, and the Asia-Pacific region. Also interviewed were 100 senior investors from global firms that manage at least $100 billion in assets.

However, regardless of their location, CEOs, board directors and institutional investors cited national and corporate gaps in cybersecurity as the biggest threats to business growth and the global economy. Income inequality and job losses stemming from technological change came second and third in the list of threats, while ethics in artificial intelligence and climate change respectively rounded out the top five.

The cybersecurity finding has far-reaching and disruptive implications for the future of work, consumer trust and government regulation.

"Future corporate growth depends on trust, whether between corporations and customers, people and technology, or management and employees. The increasing risk of cyber-attacks and the failure to find the right balance of digital and human in the workplace damages trust in all these critical dimensions," says Gil Forer, EY Global Markets Digital and Business Disruption Lead Partner.

While the risks are very real, the study found that CEOs aren't fazed. They actually see more upside in taking action to address and solve these global challenges. Half of the chief executives believe the top-tier players are obliged to do their part because, in many cases, not doing so could spell disaster.

"The world's largest companies have to be engaged," says Bala Swaminathan, Asia Advisory Board member for Westpac Banking Corporation. "It's not whether you grow or you don't grow. It's a question of whether you exist or you don't exist."

Two-thirds of the CEOs surveyed reported that they were likely to speak out publicly about the biggest problems facing the world.

"We have arrived at a tipping point in corporate action on global challenges which will have a powerful impact. The world's largest companies are set to undertake a range of meaningful actions to address global challenges such as income inequality, the ethics of AI, cybersecurity, and climate change," the report said.

Most of the CEOs surveyed say they're tweaking their corporate missions to place greater emphasis on targeting societal problems. Directors are also looking at partnering with governments or non-government organizations (NGOs). Just under half of the respondents had implemented a corporate reporting framework that included non-traditional values or were active members of industry coalitions.

C-suite is ill-prepared to meet coming demands

The long list of internal challenges starts at the top. Only one-third of respondents (34%) believe the current C-suite model is ready to meet the demands and opportunities of the next decade. But many CEOs and boards have been working to change this by adding new positions such as chief innovation officer, chief digital officer and chief strategy officer.

But further changes are in the works. Some 72% of CEOs expect to add new positions or change C-suite roles. Some 82% of boards say the same thing.

Investors want long-term value more than short-term returns

In the survey, investors also ranked the incorporation of global challenges into corporate mandates as their number-one priority for CEOs. Almost half (43%) said that a CEO's top priority should be to link internal governance, performance measures and rewards to solutions to the most pressing problems plaguing the modern world.

Investors are also paying more attention to how companies respond to global challenges and to the degree to which the company actually dedicates resources to global problem-solving., The lion's share of investors (60%) back long-term investments that tackle global challenges, if these investments take a bite out of near-term performance.

Read the rest here:

https://www.cio.com/article/3433265/lack-of-cybersecurity-is-the-biggest-economic-threat-to-the-world-over-the-next-decade-ceos-say.html

ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce

Additional photographs are available on the ISSA-COS.ORG website.

WWW.ISSA-COS.ORG

The Information Systems Security Association (ISSA) ® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?

We are always looking for articles that may be of interest to the broader Colorado Springs cyber community.

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Chapter Officers:

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: **Vacant**
- Deputy Treasurer: Vacant

Recorder/Historian: Mike Daetwyler
- Deputy: **Vacant**

Dir. of Professional Outreach: Katie Martin
- Deputy: **Vacant**

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: David Reed
- Deputy: Melissa Absher

Vice President of Training: Mark Heinrich
- Deputy: Jeff Tomkiewicz

Member at Large: James Asimah
Member at Large: Bill Blake
Member at Large: Jim Blake
Member at Large: **Vacant**

Committee Chairs:

Training: Mark Heinrich
Hospitality: Stephen Parish
Mentorship Committee Chair: Carissa Nichols
Ethics: Timothy Westland
Recognition: **Vacant**
Media: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

Executive Assistant: Andrea Heinz

** Executive Board Members*

Significant Interest Group Leads:

Chair: Anna Parrish
Women in Security : June Shore
Young Prof. in Security: Jeremiah Walker
Educators in Security: **Vacant**
Executives in Security: **Vacant**
Finance in Security: **Vacant**
Healthcare in Security: Dennis Schorn
Retail in Security: **Vacant**
DoD in Security: Steven Mulig

Past Senior Leadership

President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Past President: Pat Laverty
Past President: Frank Gearhart
Past President: Cindy Thornburg
Past President: Colleen Murphy

How a 'NULL' License Plate Landed One Hacker in Ticket Hell

By Brian Barrett, Gizmodo, August 13, 2019

Joseph Tartaro never meant to cause this much trouble. Especially for himself.

In late 2016, Tartaro decided to get a vanity license plate. A security researcher by trade, he ticked down possibilities that related to his work: SEGFAULT, maybe, or something to do with vulnerabilities. Sifting through his options, he started typing "null pointer," but caught himself after the first word: NULL. Funny. "The idea was I'd get VOID for my wife's car, so our driveway would be NULL and VOID," Tartaro says.

Read the rest here:

https://www.wired.com/story/null-license-plate-landed-one-hacker-ticket-hell/

Published at no cost to ISSA Colorado Springs by Sumerduck Publishing ™, Woodland Park, Colorado