ISSA Information Systems Security Association Colorado Springs Chapter

WWW.ISSA-COS.ORG

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 12 DECEMBER 2019

2019 is Almost Gone

A Note From Our President

By Mr. Ernest Campos

Fellow Members of ISSA-COS,

It is incredible how quickly the year has passed. It seems like just yesterday the year began and now I suddenly have visions of sugar-plums dancing in my head. As I reflect on the year soon over, I am amazed at how much our chapter accomplished. During the year, we delivered on all our scheduled chapter meetings, mini seminars, certification reviews, and conferences. Most events experienced considerable growth in registration and attendance. Yes, we experienced a few challenges along the way but, we grew from those experiences and we will use them to improve the quality of our future events.

Looking back at November, our chapter enjoyed lunch and dinner presentations provided by **Mr. Bob Gemignani**, Director of the **Pikes Peak Business and Education Alliance (PPBEA)**. Mr. Gemignani shared with us the efforts underway by PPBEA to educate folks on the labor shortage and skills gaps in cybersecurity workforce, the importance of building our own regional cybersecurity workforce right here in Colorado Springs, ways we can work together to increase cyber capacity at the community level, and how K-12 education can be a part of the workforce development solution for employers. Both these events included lots of discussion, questions, and knowledge sharing among the presenter and the attendees. Most folks expressed appreciation for the information shared and inquired as to how they can become more active in the community. As a result, our Director of Certifications is exploring ways to award Continuing Professional Education (CPE) points for those who volunteer to support PPBEA. More information will follow in 2020.

At the monthly Mini Seminar, we enjoyed dual presentations. First up was **Mr. Andrew B. Jones** who spoke to us about Application Container Security. The second presenter was **Mr. Steve Beaty** who provided a robust overview of the Cybersecurity Maturity Model Certification (CMMC) process poised to replace/augment the NIST 800-171 compliance standard. CMMC includes five different certification levels and five different protocols. Mr. Beaty provided a deep dive on all five levels and gave examples of the types of companies that would fall into each level. CMMC will be a hot topic in 2020 so, we will look to provide

(Continued on page 4)

1.2 Billion Records Found Exposed Online in a Single Server

By Lily Hay Newman, Wired, November 22, 2019

For well over a decade, identity thieves, phishers, and other online scammers have created a black market of stolen and aggregated consumer data that they used to break into people's accounts, steal their money, or impersonate them. In October, dark web researcher Vinny Troia found one such trove sitting exposed and easily accessible on an unsecured server, comprising 4 terabytes of personal information—about 1.2 billion records in all.

While the collection is impressive for its sheer volume, the data doesn't include sensitive information like passwords, credit card numbers, or Social Security numbers. It does, though, contain profiles of hundreds of millions of people that include home and cell phone numbers, associated social media profiles like Facebook, Twitter, LinkedIn, and Github, work histories seemingly scraped from LinkedIn, almost 50 million unique phone numbers, and 622 million unique email addresses.

"This data exposure is just the latest in a seemingly endless string of large-scale discoveries.."

"It's bad that someone had this whole thing wide open," Troia says. "This is the first time I've seen all these social media profiles collected and merged with user profile information into a single database on this scale. From the perspective of an attacker, if the goal is to impersonate people or hijack their accounts, you have names, phone numbers, and associated account URLs. That's a lot of information in one place to get you started."

Troia found the server while looking for exposures with fellow security researcher Bob Diachenko on the web scanning services BinaryEdge and Shodan. The IP address for the server simply traced to Google Cloud Services, so Troia doesn't know who amassed the data stored there. He also has no way of knowing if anyone else found and downloaded the data before he did, but notes that the server was easy to find and access. WIRED checked six people's personal email addresses against the data set; four were there and returned accurate profiles. Troia reported the exposure to contacts at the Federal Bureau of Investigation. Within a few hours, he says, someone pulled the server and the exposed data offline. The FBI declined to comment for this story.

The data Troia discovered seems to be four data sets cobbled together. Three were labeled, perhaps by the server owner, as coming from a data broker based in San Francisco called People Data Labs. PDL claims on its website to have data on over 1.5 billion people for sale, including almost 260 million in the US. It also touts more than a billion personal email addresses, more than 420 million LinkedIn URLs, more than a billion Facebook URLs and IDs, and more than 400 million phone numbers, including more than 200 million valid US cellphone numbers.

PDL cofounder Sean Thorne says that his company doesn't own the server that hosted the exposed data, an assessment Troia agrees with based on his limited visibility. It's also unclear how the records got there in the first place.

"The owner of this server likely used one of our enrichment products, along with a number of other data-enrichment or licensing services," says Sean Thorne, cofounder of People Data Labs. "Once a customer receives data from us, or any other data providers, the data is on their servers and the security is their responsibility. We perform free security audits, consultations, and workshops with the majority of our customers."

Troia thinks it's unlikely that People Data Labs was breached, since it would be simpler to just buy data from the company. An attacker on a budget could also sign up for a free trial that PDL advertises, offering 1,000 consumer profiles per month. "One thousand profiles to 1,000 burner accounts and you've got pretty much all of it," Troia points out.

One of the other data sets is labeled "OXY," and every record in it also contains an "OXY" tag. Troia speculates that this may refer to Wyoming-based data broker Oxydata, which claims to have 4 TB of data, including 380 million profiles on consumers and employees in 85 industries and 195 countries around the world. Martynas Simanauskas, Oxydata director of business-to-business sales, emphasized that Oxydata hasn't suffered a breach and that it does not label its data with an "OXY" tag.

Read the rest here:

https://www.wired.com/story/billion-records-exposed-online/

Membership Update

I am stepping down as the Chapter's VP of Membership so this will be my last "Membership Corner". I would like to thank everyone for their support during my tenure in this position. All our membership successes have been a result of your hard work and support! I'm equally certain that you'll continue to provide that same level of support to my successor.

I would also 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 November
Richard Peters

Our membership is at ~408 members as of the end of November.

Please watch the Newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter.

Thanks,

David Reed

Membership Committee Chairman

membership@issa-cos.org

Free Cybersecurity Training Now Available for U.S. Veterans

By Serjiu Gatlan, Bleeping Computer, November 11, 2019

A new and free cybersecurity training and certification program called Second Watch has been launched today by Palo Alto Networks to help U.S. veterans find new careers in cybersecurity after their military service is over.

This new initiative is designed to provide military veterans with all the online resources needed to aid them to switch to new careers in cybersecurity, a mission that perfectly matches their previous training on effectively responding to threats and preventing attacks.

"Second Watch is designed to be accessible to veterans at any level of technical expertise," said Palo Alto Networks VP and retired U.S. Army major general John Davis.

"The initiative includes the opportunity to earn certification as a Palo Alto Networks Certified Cybersecurity Associate (PCCSA), a Palo Alto Networks Certified Network Security Administrator (PCNSA) or a Palo Alto Networks Certified Network Security Engineer (PCNSE)."

The free digital learning courses provided by the company through the Second Watch initiative enable veterans to acquire cybersecurity knowledge on various topics ranging from "the basics of malware to managing a global infrastructure of Next-Gen Firewalls."

Veterans will also be able to get certified while enrolled in Palo Alto Networks' training initiative, with the skills they demonstrate during the certification process allowing them to find a position in the cybersecurity industry after finishing the program.

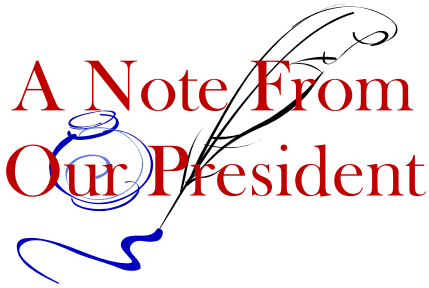
Read the rest here:

https://www.bleepingcomputer.com/news/security/free-cybersecurity-training-now-available-for-us-veterans/

(Continued from page 1)

more information on this for our members.

As for the rest of 2019, our chapter concluded the Annual Election whereby, we affirmed some new and some returning officers to our Board of Directors. All the newly elected officers were invited to attend the December Board Meeting in preparation for taking office January 1st. I am pleased to say, we will start 2020 with a full complement of principal board members. Congratulations to the following folks who were elected.



- **Michael Crandall** – Vice President
- **Scott Frisch** – Executive Vice President
- **Dennis Schorn** – Treasurer
- **Christine Mack** – Director of Communications
- **Steven Mulig** – Vice President of Membership
- **Art Cooper** – Member-at-Large (#1)
- **Jim Blake** – Member-at-Large (#2)

I also recognize and thank the following former and outgoing 2019 principal Board Members for their endearing service to our chapter. Their efforts to improve and sustain the integrity of our chapter will endure for many years to come.

- **Mark Maluschka**– Former Treasurer
- **Michael Daetwyler** – Former Recorder/Historian
- **David Reed** – Outgoing VP of Membership
- **Bill Blake** – Outgoing Member-at-Large

As this year draws to a close, I thank all of you for your strong support of our chapter, our events, and our community. Without the collective help of our **General Members**, we would not experience the success we did in 2019. During the January Chapter Meetings, I will reflect more on our accomplishments and provide a vision for 2020. It is already shaping up to be an exciting year full of great events, new opportunities, strategic partnerships, and community alliances. Please plan to attend… you won't want to miss it! With that, I am pleased to draw 2019 to a close. On behalf of our Board of Directors and Key Personnel, we wish you a happy Holiday season and a Happy New Year to come!

Sincerely,

Ernest

Cybersecurity Workforce Gap: 145% Growth Needed to Meet Global Demand

By Kevin Townsend, SecurityWeek, November 8, 2019

The biggest surprise about the cybersecurity skills gap is that it exists at all. The job description painted by the latest $(ISC)^2$ workforce study, based on responses from 3,237 existing cybersecurity professionals, is attractive.

The pay is good -- especially if you have professional certifications (average $90,000 in North America, and $58,000 in Europe). Motivation is also high: "high demand, the ability to work in a continuously evolving field, the ability to constantly solve puzzles and never get bored, and job security. A strong majority -- 65% -- intend to work in cybersecurity for the rest of their careers," states $(ISC)^2$ in its new Cybersecurity Workforce Study, 2019.

The purpose of this year's study differs slightly from earlier studies. It doesn't merely attempt to assess the workforce gap, but also seeks to assess the number of cybersecurity professionals currently in employment. The workforce gap is calculated from the hiring organizations times their expected headcount minus the current supply.

$(ISC)^2$ asserts that these two sets of figures (the current gap and the current number employed) provide a better understanding of what is required to succeed in the cybersecurity age. "We know," for example, it says, "that the global cybersecurity workforce needs to grow by 145% to meet the demand for skilled cybersecurity talent. In the U.S. specifically, it needs to grow 62%."

Read the rest here:

https://www.securityweek.com/cybersecurity-workforce-gap-145-growth-needed-meet-global-demand

DOD Looks to Increase Cybersecurity from Commercial Satellite Providers

By Shaun Waterman, Air Force Magazine, November 14, 2019

A new report by University of Minnesota researchers indicates cyberattacks pose a rising threat to food production and safety.

Commercial satellite providers seeking to sell their services to the US military will soon have to get third party certification that they are meeting cybersecurity standards, according to Air Force officials and industry executives.

The Air Force Commercial Satellite Communications Office, AFCSCO, which took over buying commercial satellite services for DOD at the end of last year, plans to have the Information Asset Pre-assessment program up and running early next year, said Andrew D'Uva, who heads the SatCom Industry Group—a trade association representing major satellite providers to the US government.

The program, known as IA Pre, was first proposed by Air Force officials last year, a spokesperson for Air Force Space Command, which houses AFCSCO, told Air Force Magazine. But moving satellite acquisition to AFCSCO from the Defense Information Systems Agency had caused delays in implementation. "This initiative is in the process of being coordinated fully," the spokesperson said, promising that "more information will be made available as the program is finalized."

IA Pre is an effort to "raise the cultural bar on cybersecurity" in the commercial satellite sector, D'Uva told Air Force Magazine. The aim is to ensure that commercial satellite services bought by the military '"will basically be at the same level" of cybersecurity as the services provided by the military's own satellites, he said.

That will enable AFCSCO to seamlessly integrate commercial services into military communications, he said. "Moving to an enterprise architecture of a mixed set of capabilities [both military and commercial] will drive resilience and better service for the warfighter," D'Uva explained.

Creating a pool of pre-certified cybersecure satcom suppliers would enable DOD to acquire those capabilities "very rapidly when required," he added.

The move comes amid growing concerns that US adversaries could use online attacks to blind or cripple commercial satellites on which the US military increasingly relies.

"Commercial satellites do not require the same level of [cybersecurity] governance as satellites in the DOD and civilian [government] sectors, and they do not have standardized security," according to a recent report about cybersecurity for satellites from the Aerospace Corp.—a non-profit that advises the government on complex space enterprise and systems engineering problems.

D'Uva welcomed the new IA Pre program, which he said would reward companies that invested in cybersecurity. Costly cybersecurity measures are hard to sustain "if your investments aren't valued," he said.

Satellite providers had made "a ton of investments" in cybersecurity and were "well-postured" to meet the new requirements, he said. He added that AFCSCO had been consulting with industry about the planned rules.

Currently the government "allows industry to self-certify, self-assess, and … in the commercial satcom area at least, they haven't bothered to check the effectiveness of those controls. It's a paper game," D'Uva said.

IA Pre will require commercial satcom providers to implement security controls on their IT systems based on a catalogue produced by the National Institute for Standards and Technology, or NIST, known as Special Publication 800-53. The controls in 800-53 are mandatory in federal agencies and cover three different levels: Low impact, medium impact, and high impact—the most secure. Satcom providers will have to implement the high impact level controls, "plus a space overlay [of additional controls] for space vehicles," D'Uva said.

Read the rest here:

https://www.airforcemag.com/DOD-Looks-to-Increase-Cybersecurity-from-Commercial-Satellite-Providers/

DoD Asks: Who Really Wrote Your Code?

US programmers routinely borrow code from all over – including Russia and China. The Pentagon is developing and buying tools to track that.

By Sydney J. Freedberg, Jr, Breaking Defense, November 12, 2019

CYBERCON: Just because you bought software from a US company, that doesn't mean all the code was written here, federal officials warned here this morning.

Software developers routinely subcontract work to foreign firms, download tools from open-source libraries, or just copy-and-paste lines of code from existing software – without checking who originally wrote what or even understanding it actually works.

The resulting rise of bugs and backdoors in recycled code is so worrying to the Pentagon that it's developing tools to track down where software really came from.

"I hope to pilot something in FY '20," said Michele Iversen, a former NSA and Army officer who's now the director of risk assessment and operational integration for the Pentagon's Chief Information Officer, Dana Deasy. That said, Iversen told reporters on the sidelines of the Fifth Domain CyberCon conference here, "we're under a continuing resolution so everything is a little bit [unclear] when we get money."

What Iversen is talking about is a "decision support tool." In essence, she wants to buy software that tells you whether software you want to buy is trustworthy. So, the question is, who watches the watchmen? How do you ensure the vetting system is itself well-vetted?

"There's a plethora of commercially available capabilities out there," Iversen said. She and her staff spent a whole "market analysis day" recently meeting with potential vendors and still didn't get to see everyone they wanted.

It turns out there's a whole emerging industry of reputable private-sector companies with "amazing" capabilities to trace your supply chain down tier after tier to the smallest building blocks, Iversen said. Better yet, she added, these firms are doing this due diligence by combing through publicly available data, which anyone can cross-check, and which can be very revealing if you look in the right places – and which you can share freely across the Defense Department without violating any security regulations.

But these private-sector services aren't free. "I have seen program offices buy some of these tools themselves," Iversen said, and her office is working on pilot projects on supply chain security with multiple acquisition programs. But small acquisition efforts with limited budgets, manpower, and time – especially when they're trying to move fast to acquire something constantly changing, such as software – can't afford high-end vetting services on their own.

So Iversen's idea, which is still evolving, is essentially for the Pentagon CIO shop to subscribe to one or more of the leading vetting services, then provide at least basic information on demand to all comers from across the Defense Department. Which services they'll use is TBD – "obviously this will be a competitive bid," Iversen said – but it's more attractive to go with companies that charge you for each piece of software you want to vet, rather than for each user that gets the vetting information, because the Defense Department will have lots of users asking about the same programs.

The decision tool will focus on widely used, commercially available "commodity products" rather than customized software purpose-built for major programs, Iversen said. "When you're doing something like purchase cards or doing simplified acquisitions, you can go to this service and be able to look up something and say, oh, Market Leader #1 has this provenance; Market Leader #2, here's its provenance."

Read the rest here:

https://breakingdefense.com/2019/11/dod-asks-who-really-wrote-your-code/

Russia internet: Law introducing new controls comes into force

By Staff, BBC, November1, 2019

A law introducing new controls on the internet has come into force in Russia amid concerns it may be used by the government to silence its critics.

In theory, the "sovereign internet" law gives officials wide-ranging powers to restrict traffic on the Russian web.

The Kremlin has said the law will improve cyber security. A spokesman said users would not notice any change.

Critics fear the Kremlin will try to create an internet firewall similar to that in China.

Experts say it is unclear how the powers of the controversial law might be used, or how effectively they can be implemented given the technology challenges and high costs.

What's the law about?

It gives the Kremlin the possibility to switch off connections within Russia or completely to the worldwide web "in an emergency". It is up to the government to decide what constitutes a threat and what actions should be taken.

The law requires internet service providers to install network equipment - known as deep packet inspection (DPI) - capable of identifying the source of traffic and filter content. In practice, this will allow the country's telecommunications watchdog Roskomnadzor to be more effective at blocking sites.

Russia is seeking to route the country's web traffic and data through state-controlled points, reducing reliance on foreign servers over which it has less control. Supporters say this is to protect the system from attacks from abroad.

To help with this project, the country is working on developing its own net address books so it can operate almost autonomously, although this work will not take effect until 2021.

US intelligence has said Russia used the internet to interfere in the US 2016 presidential election, an allegation Moscow denies.

This is the latest in a swathe of tougher internet laws approved by Russia. Earlier this year, parliament passed two bills outlawing "disrespect" of authorities and the spread of what the government deemed to be "fake news".

All the official talk is about how this law will ensure Russia keeps functioning if the West "attacks" and cuts the country off from the internet. That is why it is dubbed the "sovereign internet" bill: to underline how Russia can survive in isolation - even thrive, as it claims it has under Western sanctions.

All the chatter, though, is that the law actually aims to increase control over the internet here inside Russia. The DPI technology being tested allows the state regulator to filter traffic and block what it wants. The criteria for such censorship is usefully vague.

The hugely popular messaging app Telegram will likely be an early target. The regulator's last attempt to block it using IP addresses was a flop as hundreds of other sites and service were knocked off line instead.

If the filtering technology is installed nation-wide, IT experts are sure all users will feel it. One compared the attempt to squeeze all internet traffic through the DPI "black boxes" to the crush of passengers trying to get on the Moscow metro at rush hour.

Why are there concerns?

Campaigners say the law, which was signed by President Vladimir Putin earlier this year, is an attempt to increase censorship, building on the internet legislation that already curtails freedom of expression and privacy.

"Now the government can directly censor content or even turn Russia's internet into a closed system without telling the public what they are doing or why," said Rachel Denber, Human Rights Watch's deputy Europe and Central Asia director.

The law, observers say, allows the government to block content without judicial consent and leaves users unaware about what information is being blocked and why.

Read the rest here:

https://www.bbc.com/news/world-europe-50259597

NIST Call For Comments

By Staff, NIST, November, 2019

NIST is proposing updates to its standards on digital signatures and elliptic curve cryptography to align with existing and emerging industry standards. As part of these updates, NIST is proposing to adopt two new elliptic curves, Ed25519 and Ed448, for use with EdDSA. EdDSA is a deterministic elliptic curve signature scheme currently specified in the Internet Research Task Force (IRTF) RFC 8032, Edwards-Curve Digital Signature Algorithm. NIST further proposes adopting a deterministic variant of ECDSA, which is currently specified in RFC 6979, Deterministic Usage of the Digital Signature Algorithm and Elliptic Curve Digital Signature Algorithm. Finally, based on feedback received on the adoption of the current elliptic curve standards, the draft standards deprecate curves over binary fields due to their limited use by industry.

In addition to updating NIST's Elliptic Curve Cryptography standards, Draft FIPS 186-5 proposes the removal of the Digital Signature Algorithm (DSA), noting recent security analysis against DSA implementations and increased industry adoption of ECDSA.

The proposed digital signature algorithms are included in Draft FIPS 186-5. NIST-recommended elliptic curves, previously specified in FIPS 186-4 Appendix D, are now included in Draft NIST SP 800-186.

NOTE: A call for patent claims is included on page iv of Draft SP 800-186. For additional information, see the Information Technology Laboratory (ITL) Patent Policy--Inclusion of Patents in ITL Publications.

Federal Register Notice:
https://www.federalregister.gov/a/2019-23742

Draft FIPS 186-5:
https://csrc.nist.gov/publications/detail/fips/186/5/draft

Draft NIST SP 800-186:
https://csrc.nist.gov/publications/detail/sp/800-186/draft

The public comment period for both documents ends on **January 29, 2020**. For copies of the documents and instructions for submitting comments, see the publication links below for Draft Federal Information Processing Standards Publication (FIPS) 186-5, Digital Signature Standard (DSS) and Draft NIST SP 800-186, Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters.

The State of cybersecurity in the pharmaceutical industry

Ryan Stewart, Cyware, November 25, 2019

Pharmaceutical companies face a special level of responsibility when it comes to data protection. These companies collect a wide range of data including proprietary information about patented drugs, data related to pharmaceutical advances and technologies and personal information belonging to patients.

Losing control over sensitive data can have catastrophic consequences and in turn, impact patients' and consumers' trust. A cybersecurity breach on such organizations can wreak havoc, resulting in the compromise of proprietary digital assets & private information. These types of attacks can also potentially damage the critical systems that the organization heavily relies on.

Reckoning some major attacks

One of the most significant cybersecurity attacks on a pharmaceutical company in recent history struck Merck &Co. Merck was hit massively during the NotPetya attack that occurred in 2017. The attack had disrupted its worldwide operations, forcing the company to halt the production of new drugs, and significantly impacting the company's revenue for the year. Following the attack, Merck had reportedly lost over $300 million in Q3 of 2017 alone.

Two major pharmaceutical firms - Roche and Bayer - confirmed earlier this year that they were impacted by the Winnti cyber attack, believed to be tied to the Chinese government. Fortunately, both companies reported no loss of sensitive data.

A biopharma company disclosed that a cyberattack in March 2019 harvested data from around 1% of its clients. The attack was carried out by a highly sophisticated, well-resourced intruder.

How threat actors can benefit?

Pharmaceutical companies are a treasure trove of valuable data. Cybercriminals can harvest this data to sell it on the dark web or to rival companies.

According to Proofpoint's Q3 2018 Threat Report, pharma was the number one industry targeted in email fraud attacks. As such attacks begin with penetration on the IT networks through an email phishing campaign, they could ultimately migrate to the OT network via systems accessible to both environments. If these environments are left unchecked, malware can cause unpredictable and dangerous disruption to pharmaceutical production processes.

Engaging against attacks

Cybersecurity is everyone's job. Every single employee, from the CEO to the intern in an organization, plays an important role. In addition to the C-suite working with the cybersecurity experts to craft and implement company-wide best practices, employees should also need to understand what that can do to protect their company's digital assets.

Read the rest here:

https://cyware.com/news/the-state-of-cybersecurity-in-the-pharmaceutical-industry-42835bac

ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

Blue Ribbon Trophies & Awards
245 E Taylor St (behind Johnny's Navajo Hogan on North Nevada)
Colorado Springs
(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

2020 Schedule of Events

Chapter Meetings – Dinner (5:30 – 7:30 PM)

Tuesday, January 21, 2020
Tuesday, February 18, 2020
Tuesday, April 21, 2020
Tuesday, May 19, 2020
Tuesday, July 21, 2020
Tuesday, August 18, 2020
Tuesday, October 20, 2020
Tuesday, November 17, 2020

Chapter Meetings – Lunch (11:00 – 1:00 PM)

Wednesday, January 22, 2020
Wednesday, February 19, 2020
Wednesday, April 22, 2020
Wednesday, May 20, 2020
Wednesday, July 22, 2020
Wednesday, August 19, 2020
Wednesday, October 21, 2020
Wednesday, November 18, 2020

Mini-Seminars – Breakfast (8:30 – 12:00 PM)

Saturday, January 25, 2020
Saturday, February 22, 2020
Saturday, April 25, 2020
Saturday, May 16, 2020
Saturday, July 25, 2020
Saturday, August 22, 2020
Saturday, October 24, 2020
Saturday, November 14, 2020

ISSA-COS Conferences

Cyber Focus Day (CFD) Symposium

Wednesday, March 25, 2020
Thursday, March 26, 2020

Peak Cyber (PC) Symposium

Wednesday, September 16, 2020
Thursday, September 17, 2020
Friday, September 18, 2020

Security + CE Reviews

Saturday, March 7, 2020
Saturday, March 14, 2020
Saturday, March 21, 2020
Saturday, September 12, 2020
Saturday, September 19, 2020
Saturday, September 26, 2020

CISSP Review

Friday, June 5, 2020
Saturday, June 6, 2020
Saturday, June 13, 2020
Friday, June 19, 2020
Saturday, June 20, 2020
Saturday, June 27, 2020

CyberVIEW Hiring & Networking Fairs (1:00 – 6:00 PM)

Wednesday, March 11, 2020
Wednesday, June 10, 2020
Wednesday, September 9, 2020
Wednesday, December 9, 2020

CyberVIEW hiring and networking events connect Cybersecurity professionals searching for employment with companies looking to fill current or upcoming positions. Soft-skill coaches and resume reviewers will be on hand. This event concludes with a social hour for exhibitors, ISSA-COS members, and guests.

Annual Chapter Celebration (11:00 – 1:00 PM)

Thursday, December 3, 2020

Take time with ISSA-COS to reflect and celebrate the many accomplishments of our chapter from through-out the year. During this event, we will present specific honors, introduce the newly elected board members, and recognize specific professional accomplishments of our general members.

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

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 (WIS)**
- Young Professional in Security – **Y**[oung Professionals]**IS (YIS)**
- Educators in Security – **E**[ducators]**IS (EduIS)**
- Executives in Security – **E**[xecutives]**IS (EIS)**

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 (FIS)**
- Healthcare in Security – **H**[ealthcare]**IS (HIS)**
- Retail in Security – **R**[etail]**IS (RIS)**
- DoD in Security – **D**[oD]**IS (DodIS)**

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.

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

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

ISSA-COS Scholarship Fund Sponsor—ASPG
https://aspg.com/

ASPG
Advanced Software Products Group, Inc.

Update Your Profile!

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

Ongoing Research Project Examines Application of AI to Cybersecurity

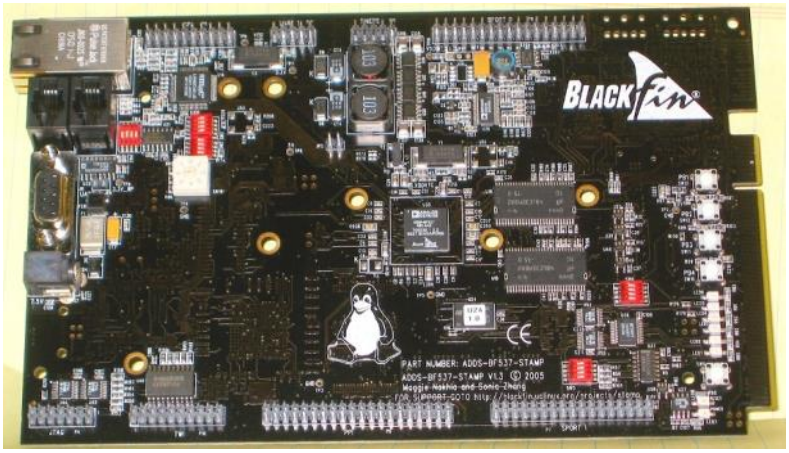
By Kevin Townsend, SecurityWeek, November 21, 2019

Project Blackfin is ongoing artificial intelligence (AI) research challenging the current automatic assumption that deep-learning neural network principles are the best way to teach a system to detect anomalous behavior or malicious activity on a network. Run by security firm F-Secure, the project is examining the alternative applicability of distributed swarm intelligence in decision making.

"People's expectations that 'advanced' machine intelligence simply mimics human intelligence is limiting our understanding of what AI can and should do," explains Matti Aksela, F-Secure's VP of artificial intelligence. "Instead of building AI to function as though it were human, we can and should be exploring ways to unlock the unique potential of machine intelligence, and how that can augment what people do."

Project Blackfin is being run by F-Secure with collaboration between in-house engineers, researchers, data scientists and academic partners. "We created Project Blackfin," continued Aksela, "to help us reach that next level of understanding about what AI can achieve." Although it is a long-term project, some early principles are already being incorporated into F-Secure's own products.

The primary problem with many current anomaly detection AI systems is well-known: too many false positives or too many false negatives. This is difficult to solve simply by the nature of how the systems work. Streams of data from endpoints and network traffic are centralized and analyzed on arrival, and then stored for later audit or forensic analysis. Because the data arrives from multiple sources it is difficult to correlate events across multiple sources. Since attackers often build delays into their attacks, new events may also need to be related to historical events to be able to contextualize possibly malicious activity.



The result is that finding the best sensitivity settings for detection of behaviors is critical. Set high to ensure nothing is missed results in huge numbers of false positives that need to be manually triaged by the security team. Set too low to reduce the false negatives increases the potential for false positives.

Blackfin is exploring the use of distributing the AI as agents within each endpoint and server of a network in a collaborative manner. That intelligence becomes expert in the acceptable use of its own host. The model is inspired by the patterns of collective behavior found in nature, such as the swarm intelligence found in ant colonies or schools of fish. "The project aims to develop these intelligent agents to run on individual hosts," says F-Secure. "Instead of receiving instructions from a single, centralized AI model, these agents would be intelligent and powerful enough to communicate and work together to achieve common goals."

Consider the machine learning predictive text input capabilities of individual phones. They learn the text habits of their owners very quickly, being able to rapidly offer probable word completions based on their owners' habits. This is the type of distributed intelligence being explored by Blackfin, with the intelligence located in the device -- but with the added ability for each intelligence to collaborate with the intelligence of adjacent intelligences. What may be just suspicious activity in the context of one endpoint can be confirmed as malicious or benign in the context of its action on adjacent endpoints -- each of which has its own endpoint-specific intelligence.

This improves the correlation and contextualization of suspicious activity since the event is immediately, in situ, seen in the context of both the source and destination hosts. In our phone example, it might be equivalent for the text input intelligence on one phone being able collaborate with the destination intelligence and say, 'Stop. You should not use that language with your grandmother.'

"Essentially," said Aksela, "you'll have a colony of fast local AIs adapting to their own environment while working together, instead of one big AI making decisions for everyone."

Read the rest here:

https://www.securityweek.com/ongoing-research-project-examines-application-ai-cybersecurity

Too Many CISOs Delay Cyber Response, DHS Official Says

By Jack Corrigan, NextGov, November 19, 2019

An overabundance of cybersecurity leaders across federal agencies is hindering the government's ability to adapt to the changing digital landscape, according to a top Homeland Security Department official.

Agencies must be able to act swiftly to keep their tech ecosystems secure against a constantly evolving array of digital threats, but excessive bureaucracy within the federal cyber community is impeding that quick action, according to Mark Bristow, director of the hunt and incident response team within Homeland Security's National Cybersecurity and Communications Integration Center. Though it's critical to have different groups weigh in on cybersecurity policies, he said, today there are too many cooks in the kitchen to execute a coherent, unified strategy.

"We have too many [chief information security officers] in the government," Bristow said Tuesday at the Cyber Summit hosted by *Nextgov* and *Defense One*. "I understand why they're there ... but it really gets in the way of setting strategic vision. You have all these people who have slightly conflicting guidance and opinions ... and what happens is you start to get organizational stagnation because you can't make any decisions, and therefore you can't make any progress."

And according to Bristow, adversaries are already exploiting that stagnation.

"They know that this is how this works, they count on it with their tactics and techniques," he said. "We need to flip our operational paradigm in a way that frustrates the adversary."

Bristow isn't the first federal leader to raise concerns about excess bureaucracy in the cyber community—in January, Rep. Jim Langevin, D-R.I., said congressional efforts to bolster the country's security posture are hindered by the numerous committees that want to weigh in.

But bureaucracy isn't the only organizational hurdle that limits the government's ability to rapidly respond to cyber threats.

The high turnover among agency chief information officers and chief information security officers also limits agencies from executing a consistent digital strategy, according to Nick Marinos, director of the Information Technology and Cybersecurity team at the Government Accountability Office. When these executives leave, agencies not only lose institutional knowledge but they also often need to change their approach to accommodate the new leader's digital priorities.

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/11/too-many-cisos-delay-cyber-response-dhs-official-says/161403/

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

Information Systems Security Association
Colorado Springs Chapter

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:* _____

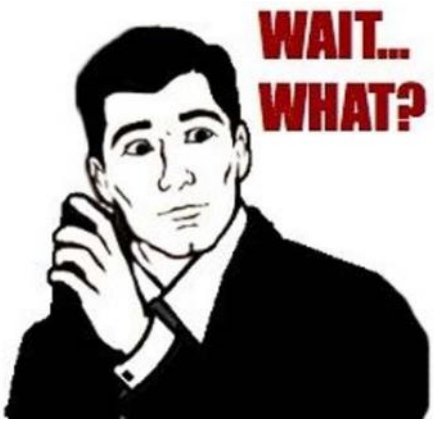
Next steps:

DISA Official: 'No One Knows' How Cyber Standards Will Impact Contractor Pool

By Jack Corrigan, NextGov, November 4, 2019

Officials at the Defense Information Systems Agency don't know whether forthcoming vendor cybersecurity standards will shrink the pool of contractors that qualify for critical tech projects.

In January, the Pentagon plans to publish the final version of the Cybersecurity Maturity Model Certification, or CMMC. Under the framework, companies would have their cyber practices graded on a scale of one to five, and procurement officials would use the rating to determine which vendors are eligible for certain contracts, with more sensitive projects requiring more stringent security standards.



While the program is intended to push vendors to strengthen their security standards and increase visibility into the department's supply chain, it could also render a significant chunk of the Pentagon's contractor pool ineligible for its most sensitive projects, according to DISA officials.

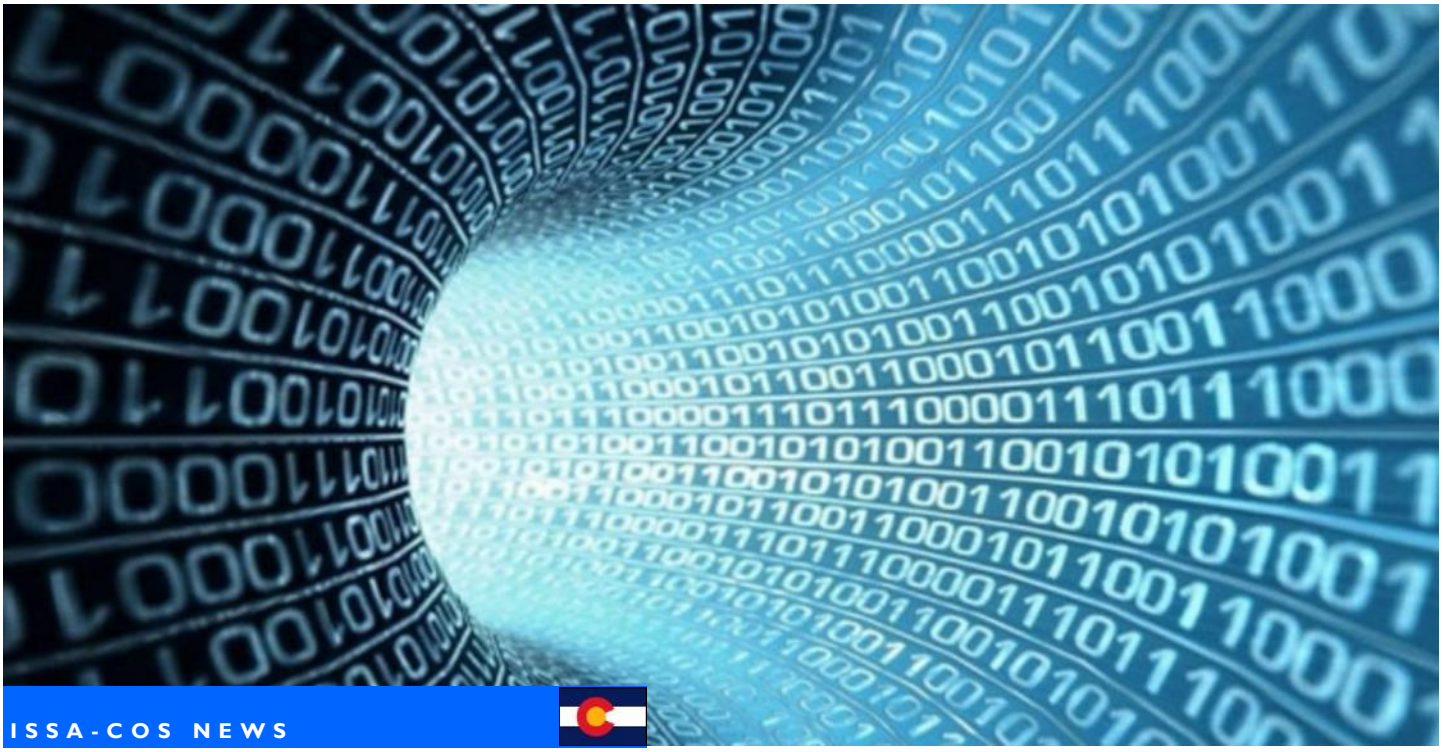
"A very small number … of the 300,000 [defense industrial base] companies have state-of-the-art cybersecurity. The majority of them are at the lower end of that one to five scale," Maj. Gen. Garrett Yee, assistant to the director of DISA, said Monday during a speech at the agency's annual Forecast to Industry Day. That notion is based on estimates from the Office of the Secretary of Defense, not DISA's own assessment, he noted.

When asked during a media roundtable how the program would impact the pool of qualified vendors for the agency's sensitive tech projects, Yee said, "No one knows the answer to that."

Small businesses make up a significant percentage of the department's contractor pool, and many of those firms haven't historically devoted as many resources to standing up robust cyber defenses, according to Yee. The certification is meant to be both "affordable" and "achievable" for small businesses, he said, though the Pentagon received many questions about how small businesses would compete with larger vendors under the new model.

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/11/disa-official-no-one-knows-how-cyber-standards-will-impact-contractor-pool/161069/



The 404 Error Was an obvious Innovation, Yet The Internet You Know and Love Wouldn't Be Possible Without It

By Jesse Dunietz, Popular Mechanics, October28, 2019

It's the bane of every web surfer, the internet's version of fingernails on the chalkboard. Click almost any link that dates back to pre-2005 and brace for the inevitable: "HTTP 404 Not Found."

Anyone who's spent time near an internet connection is familiar with the 404 error, a webserver's way of saying you've reached a dead end. What's less well known is that this very error is what allowed the World Wide Web to exist in the first place.

The History of Hyperlink

Let's talk about hyperlinks. We tend to think of the vast array of linked pages we call the web as an outgrowth of internet connectivity. To put it another way: First came the communication network that allows computers to exchange data, and then on top of it we built an interconnected maze of documents, cat videos, etc. In fact, the contrary is correct. The idea of hypertext, or text with followable links to other content, predates networked computers by *decades*.

Hypertext dates back at least to 1945, when technology pioneer Vannevar Bush proposed a hypertext-augmented microfilm machine which he dubbed the "Memex." Bush envisioned a strip along the edge of the microfilm where, at the user's instruction, the memex could stamp the address code of a related film panel. Any time thereafter, someone viewing the same piece of microfilm could instantly pull up the linked panel.

Bush was so far ahead of his time that his ideas remained pie-in-the-sky dreams until the 1960's. With digital computers taking off, real hypertext soon became a reality. IT legend Ted Nelson drew on Bush's ideas for a wildly ambitious hypertext concept called Project Xanadu, though it didn't come to even partial fruition until 1998. In the late '60s, though, Nelson did co-develop a less elaborate hypertext system that supported links within a document.

At the same time, Douglas Engelbart, one of the early greats in human-computer interaction, was working on his revolutionary NLS (oNLine System). Among NLS' many groundbreaking features was the fact that the system allowed users to jump around within a document using hyperlinks. Between the work of Nelson, Engelbart, and their successors, hypertext systems were already hanging around in the mid-1980s.

The Modern Web Takes Shape

These systems came with limitations, the biggest being that they were limited to single computers. For example, Apple's HyperCard maintained a database of note cards that could link only to other cards on the same device. But with the rise of computer networks, links from documents on one computer to documents on another were a natural extension. Even so, it wasn't until 1989 that CERN contractor Tim Berners-Lee invented the World Wide Web.

"The frustration was that there's all this unlocked potential," Berners-Lee said in 2009 during a TED talk remembering his HTTP creation. "On all these disks, there were documents. Imagine all this being part of some big virtual documentation system in the sky, say, on the internet, then life would be so much easier."

But for this idea to take root on a large scale, something was missing. That something was the 404 error.

Before Berners-Lee came along, hypertext systems typically made sure that every link led somewhere. All new links would be added to a centralized database of documents and links. If the link's target was changed or deleted, the database had to update the link accordingly.

Keeping the hyperlinks consistent was very helpful for the user. It was also easy enough to do when all the data resided on a single computer or small network. But in a large network of computers, you'd need one central authority where all documents and links would be registered. There wasn't a database in existence that could handle continuously updating every single link the world over.

For a while, this issue received little attention. Most researchers were still focused on notecards, help applications, and other small-scale systems. A few projects did allow one-way links from one machine to another without a central authority, but they still assumed that these links would be maintained as part of a team's cohesive document authoring process.

Turns out, there was a much simpler answer.

The Birth of "404 Not Found"

Read the rest here:

https://www.popularmechanics.com/technology/a24091/404-error-world-wide-web/?utm_source=pocket-newtab


November 2019
Chapter
Meetings
ISSA
Information Systems Security Association
Colorado Springs Chapter


WHITE RIVER
BUDDHIST TEMPLE

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.

Chapter Officers:

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

Recorder/Historian: Andrea Heinz
- 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: Phebe Swope

Member at Large: Bill Blake
Member at Large: Jim Blake
Member at Large: James Asimah
Member at Large: Dennis Kater

Committee Chairs:

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

Executive Assistant: Andrea Heinz

** Executive Board Members*

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

Past Senior Leadership

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

Now even the FBI is warning about your smart TV's security

By Zach Whittaker, TechCrunch, December 1, 2019

If you just bought a smart TV on Black Friday or plan to buy one for Cyber Monday tomorrow, the FBI wants you to know a few things.

Smart TVs are like regular television sets but with an internet connection. With the advent and growth of Netflix, Hulu and other streaming services, most saw internet-connected televisions as a cord-cutter's dream. But like anything that connects to the internet, it opens up smart TVs to security vulnerabilities and hackers. Not only that, many smart TVs come with a camera and a microphone. But as is the case with most other internet-connected devices, manufacturers often don't put security as a priority.

Read the rest here:

https://techcrunch.com/2019/12/01/fbi-smart-tv-security/

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