WWW.ISSA-COS.ORG

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 7 JULY 2019

Summer is Here!

ISSA-COS Members,

Welcome to Summer! As we kick-off the months of July and August, we can look forward to another round of monthly chapter meetings and mini seminars. During the summer months attendance tends to dip a little so I ask all of you to seriously consider attending our events. Participation is important and helps add value to the time our guest speakers donate to our chapter.

During the month on June, we had the honor of sponsoring the M2 Technologies/HP Enterprise Artificial Intelligence (AI) Workshop. This event included two identical sessions; an AM session held on Peterson Air Force Base and a PM session held at M2 Technologies Headquarters. Both events were well attended, and the presentations were very informative. Our chapter was invited to provide announcements and we issued CPE forms to the attendees.

On the horizon is our 9th Annual Peak Cyber Symposium scheduled for September 3rd, 4th, and 5th. Once again, we will meet up at the Double Tree Hotel in Colorado Springs. This year's event is shaping up to be another incredible year. SPLUNK! Is returning as our Capture-the-Flag (CTF) sponsor and facilitator. In 2018, we had 23 CTF participants. This year we are looking reach 55 participants. If you have never participated in a CTF event, this is the right place to start. All levels of simple and complex challenges will be presented. The event will include lunch and plenty of energy drinks!

Also added to this year's symposium is a special dinner event on the evening of the Sep. 3rd. Although the conference is still free to attend for members, the dinner event will cost. This will be a plated dinner event with salad, entrée and dessert and will include presentations of special awards and a Keynote Dinner Speaker. Tickets for the dinner event are only $55 so, please register early to guarantee your seat!

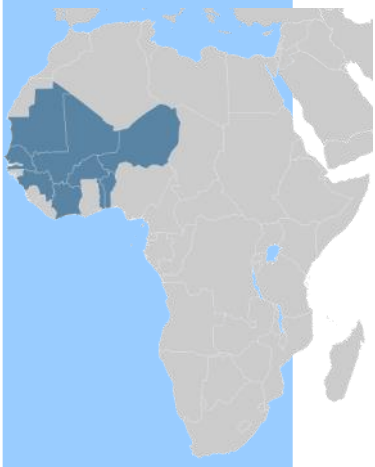
Each year, we send out a request for volunteers to help support our Peak Cyber symposium. We typically need folks to work the check-in table, our ISSA-COS booth, and to serve as event jockeys ensuring our breakout sessions run smoothly. A call for volunteers will be released in July. Please consider stepping up and helping. Our

(Continued on page 4)

A Note From Our President

By Mr. Ernest Campos

Inside the Operations of a West African Cybercrime Group



"The preferred attack is the one that nets the highest return as quickly as possible, and victims are milked for every penny possible."

By Kevin Townsend, SecurityWeek, June 5, 2019

Following an unsuccessful business email compromise (BEC) attack against a security firm, researchers have used active defense techniques to gain unprecedented insight into a Nigerian scamming group. The initial attack purported to be an email from the firm's CEO asking the CFO to instigate "a domestic wire transfer to a vendor."

Over the last few years, BEC has become one of the most profitable of all cybercrimes. The latest report from the FBI's Internet Crime Complaint Center (IC3) for 2018 states that 20,373 victims lost a total of $1.3 billion to BEC. This was the single largest category of reported internet crime, representing approximately 48% of the total losses of $2.7 billion. However, the remaining $1.4 billion loss clearly demonstrates that BEC is not the only con in town.

The Agari Cyber Intelligence Division (ACID) engaged with the BEC scammer seeking to defraud Agari. What it discovered is a criminal organization that started from a single Nigerian criminal entrepreneur (who they call Alpha) in 2008 and developed into a complex organization of at least 35 actors today. ACID calls this group Scattered Canary, and demonstrates that BEC is just one of many types of fraud perpetrated by the gang. BEC does not stand alone from the other online frauds that comprised 52% of IC3's reported losses in 2018, and may well -- as in the case of Scattered Canary -- be directed by the same criminal group.

"We were able to map out dozens of relationships," say the researchers, "an entire infrastructure, thousands of email discussion threads, hundreds of romance and fraud victims, dozens of scam kits, and other evidence that helps connect the dots between a wide universe of threat actors and actions associated with this West African fraud ring."

Alpha started his criminal career with early Craigslist scams, being mentored by a more senior criminal named as Omega. This is where he learned his basic tradecraft in social engineering. But he always aimed high. During the first 15 months, Alpha delivered more than 100 addresses to Omega, who was responsible for sending the fake checks to victims -- typically in the $2,000 to $4,000 range. The desire to maximize profits may lie behind the continuous expansion of Alpha's organization, and its move towards larger targets and more profitable scams.

Alpha's first diversification, in 2010, was into romance scams. Romance fraud taken together with confidence fraud was the second most costly fraud noted by IC3, with reported losses of $362.5 million in 2018. There is nothing romantic about romance fraud. The criminals first extract every penny possible from the victim, and then carry on using them by migrating them into mules.

'Jane' was such a victim. By 2016, her 'boyfriend' had extracted as much money as he could from her, and converted her into a mule. Over 18 months she opened five mule accounts and bought 20 prepaid cards for her boyfriend. An early password for an account was 'weare4ever'. A late password was 'iam2wornout'. Jane died in 2017; but even after her death, say the researchers, "Scattered Canary continued to victimize her. In October 2017, a member of the group attempted to take out an auto loan using Jane's personal information, providing more evidence that these groups are only interested in one thing -- money."

The romance frauds have continued even though Scattered Canary, led by Alpha, started looking at more immediately profitable targets in 2015. This started with credential phishing, largely general in nature and via a Google Docs phishing page. Towards the end of 2015, the attacks began to focus on North America and primarily the U.S. This paused in February 2016.

It restarted in March 2017, but with a new focus. Credential phishing now almost entirely focused on enterprise credentials, using phishing pages mimicking common business applications such as Adobe, DocuSign and OneDrive. Over the next 18 months, say the researchers, "Scattered Canary received more than 3,000 account credentials as a result of their phishing attacks."

Read the rest here:

https://www.securityweek.com/inside-operations-west-african-cybercrime-group

Membership Corner

Membership Update

As summer gets into full swing, we're working hard on the upcoming Peak Cyber Symposium, 3—5 September at the DoubleTree by Hilton, Colorado Springs. Attendance is free for all ISSA-COS, ISSA-Denver, and ISSA-Northern Colorado as well as anyone with a .mil, .gov, or .edu email address. This is a great opportunity to showcase our chapter so let all your colleagues know about it. It is also one of our most effective membership recruiting tools that we have. Please take a minute to register at the Federal Business Council (FBC) website at https://www.fbcinc.com/e/PeakCyber/attendeereg.aspx. Early registration gives us a big leg up when trying to recruit sponsors for the event and the chapter.

Our membership is ~450 members as of the end of June. 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.

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.

New Members June
Rebecca Botvinik
Anna Parrish
Alex Wood
Andrew Jones

Thanks,

David Reed

Membership Committee Chairman

membership@issa-cos.org

Pentagon to Unveil New Cybersecurity Maturity Model Certification (CMMC) for Defense Contractors

By Colleen Johnson, JDSUPRA, June 10, 2018

The Department of Defense announced that it is developing a new cybersecurity standard and certification for defense contractors. It is named the "Cybersecurity Maturity Model Certification" (CMMC).

Notably, the intent of the CMMC is to improve cybersecurity deficiencies in the defense industrial base and secure the supply chain.

The CMMC is expected to be based on NIST SP 800-171, as is the current Defense Federal Acquisition Regulation Supplement (DFARS) rule. Specifically, DFARS Clause 252.204-7012 requires defense contractors handling sensitive, unclassified information to implement the 110 security controls of NIST SP 800-171.

However, the CMMC may incorporate or rely on frameworks in addition to NIST SP 800-171.

According to news reports, the CMMC will serve as the enforcement mechanism lacking in the current DFARS rule.

Read the rest here:

https://www.jdsupra.com/legalnews/pentagon-to-unveil-new-cybersecurity-18009/?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

(Continued from page 1)

chapter will greatly appreciate your support.

Throughout our community, several events are taking place of interest to IT and Cybersecurity professionals. In the months to come, we hope to begin adding these events to our own Calendar of Events on our website. If you come across events you believe other member would be interested in attending, please send us the information and a registration link to info@issa-cos.org and we will add it to our calendar.

Last of all, our board of directors is announcing the opportunity for general members to observe our monthly board meetings. We will even reserve two speaking slots for general members to address the board on a topic of their choice. Invitations to attend and to reserve a speaking slot will be released starting in July. We look forward to seeing you there! As always, we thank you for your support and for helping make our chapter the best it can be.

A Note From Our President

Sincerely,

Ernest

Call for Articles: "Best of ISSA-COS" 2019

- Network and Infrastructure Security
- Web Security
- Endpoint Security
- Application Security
- Managed Security Service Providers
- Data Security
- Mobile Security
- Risk and Compliance
- Identity and Access Management
- Security Operations and Incident Response
- Threat Intelligence
- IoT
- Messaging Security
- Digital Rights Management
- Security Consulting
- Blockchain
- Fraud and Transaction Security
- Cloud Security

Deadline: August 16, 2019

Volunteer Opportunities

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

Breakfast with ISSA-COS

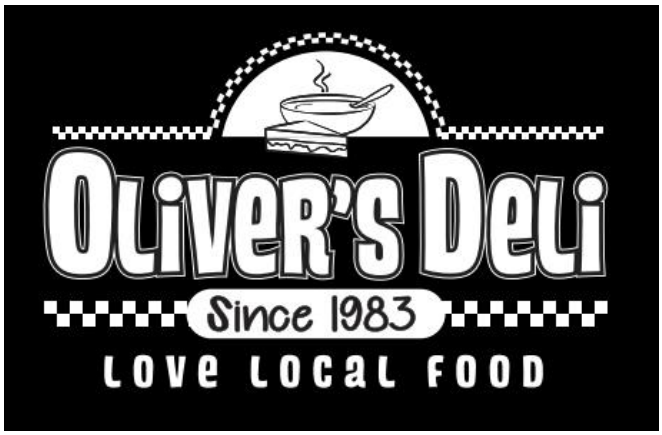
ISSA-COS will arrange for Oliver's Deli to come sell breakfast at your office!

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!



MEET THE BOARD MEMBER

As members of the Colorado Springs Chapter of the ISSA you get to enjoy a great number of benefits such as Monthly Meetings, Mini Seminars, Conferences and networking with peers. As a not-for-profit organization these things can only be accomplished thanks to the volunteers who make them happen. In this edition, we are going to highlight and get to know our chapter Vice President of Training Mark Heinrich.

Below are some questions I posed to him and his responses.

- How long have you been a member of ISSA (COS)?

  2002

- Why did you decide to join the Board for ISSA-COS?

  Want to support the organization and its goals

- Tell us something about yourself?

I'm currently a Cyber Analyst for DoD, enjoys cycling, hiking, and woodworking. Adjunct professor of Computer Science department at CTU.

- What is your experience in the Information Systems Security arena?

I started with cyber systems security on F-35, moved to trusted development on other projects, and general cyber engineering for commercial cloud-based service company.

- Do you have one "horror" story about Cyber Security you can share?

Contractor and the government civilians did not agree on contract terms but proceeded to start anyway. The result was shoddy cyber security and a hellish working environment.

- How has the Chapter helped/supported you?

  It has provided many opportunities to keep learning and to network with good people.

- How would you like to see the Chapter grow and/or expand?

I like Ernie Campos' plan to make the ISSA-COS an institution in the Springs. It would be good if we could reduce the turnover, build a bigger officer corps, and support the community more.

Mike Crandall

ISSA-COS Vice-President

Update Your Profile!

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

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/

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.

Top Cybersecurity Certifications: Who They're For, What They Cost, And Which You Need

By Roger A. Grimes, CSO Online, April 17, 2019

Two of the most common questions I'm asked are, "Is having a computer security certification is helpful in getting a job or starting a career in computer security?," and if so, "Which certification should someone get?." The answer to the first question is a definite yes. Getting a certification, while not a cumulative showing of your entire experience and knowledge in a particular area, can only help you. That's true not only in getting a new job, but in improving your knowledge and experience overall, even in your current job.

Every certification I've gained took focused, goal-oriented study, which employers view favorably, as they do with college degrees. More important, I picked up many new skills and insights into IT security while studying for each certification test. I learned about new things, and I also gained new perspectives on subjects I thought I had already mastered. I became a better employee and thinker because of all the certifications I have studied for and obtained. You will too.

Sometimes, a particular certification is the minimum hurdle to getting an in-person job interview. If you don't have the cert, you don't get invited. Other times, having a particular certification can give you a leg up on competing job candidates who have similar skill sets and experience, but don't have the desired certification.

Security is more important to computing and the internet than ever before, and the following, well-respected security certs will not only help you stand out from the crowd, but also make you a more valuable member of the IT security community.

Here is a summary of some of the most desired IT security certifications.

Certified Information Systems Security Professional (CISSP), ISC2

The International Information Systems Security Certifications Consortium's (ISC^2) Certified Information Systems Security Professional (CISSP) certification is the most coveted and accepted computer security certification around. This general computer security knowledge certification exam covers eight Common Body of Knowledge (CBK) domains, including access control, operations security, cryptography, and more.

The test used to consist of 250 multiple-choice questions that had to be answered in under six hours, but as of December 2017, it now uses adaptive testing, which reduces the number of questions and time to take to a maximum of three hours. Candidates must already have four to five years of professional experience in two or more of the CBK domains, and they must be endorsed by a current CISSP certificate holder. Those who pass the certification must also sign and agree to follow a set of ethics, and each certification holder must periodically resubmit proof of continuing education, along with a fee, to keep the CISSP designation. Initial exam cost is $699.

SysAdmin, Networking, and Security (SANS) Institute

The SysAdmin, Networking, and Security Institute (SANS) organization and website is a great resource for security pros. Training, research, education, books, certifications -- SANS does a lot and does it well. If you're interested in being a respected technical expert, SANS offers the certs for you. It even offers two master-level accredited degrees under the brand of the SANS Technology Institute, if you want the pinnacle technical achievement of our field.

SANS has a host of certifications, ranging from very niche security topics -- malware analysis, firewalls, host security, security controls, and so on -- to its hugely respected Global Information Assurance Certification (GIAC) Security Expert designation. I don't think I've ever taken a SANS course that didn't teach me more in a few hours than in weeks spent in classes offered by other training vendors, and I've yet to meet a GIAC holder that didn't impress me.

GIAC certifications are classified in five subject areas: security administration, forensics, management, auditing, and software security. Most exams are open book and have a time limit of two to five hours. The candidate must complete the certification within four months of attempting the exam. Unfortunately, according to the GIAC exam guide, some tests could include "unscored" test questions like the CISSP. My guess is there will be fewer beta test questions and what they have is better proctored. SANS is starting to venture into hands-on testing that involves live virtual machines (VMs).

Some of SANS's most popular GIAC exams are GIAC Information Security Professional, GIAC Certified Incident Handler, and GIAC Reverse Engineering Malware, but it offers courses that run the gamut, including Windows, web servers, penetration testing, Unix security, wireless networking, programming, leadership, and program management. GIAC testing is meant to be taken after attending SANS training, which usually lasts a week, but you can challenge (not take the official training) the exam for $1,699. All GIAC certification exams must be renewed every four years. If you want to learn a lot about computer security, how hackers hack, and how malware is made, start your SANS courseware now.

Certified Ethical Hacker (CEH), the EC-Council

The EC-Council's Certified Ethical Hacker (CEH) certification is well-respected way to learn how to be a white-hat hacker (or professional penetration tester). The CEH introduced me to some interesting hacking tools that I still use today. The four-hour exam includes 125 multiple-choice questions. The application eligibility fee is $100.

(Continued on page 9)

(Continued from page 8)

You will sometimes hear long-time computer security professionals talking down about the CEH certification. I think that is from earlier versions when CEH was one of the first computer certifications for penetration testing, back when computer security exams, in general, were new and easier to pass. Today, the CEH holds its own for general toughness, and the EC-Council offers a number of other useful exams, including Computer Hacking Forensic Investigator, Licensed Penetration Tester, Certified Incident Handler, and Certified Disaster Recovery Professional. It even has an exam for a Chief Information Security Officer.

Offensive Security Certified Professional (OSCP)

If your hacking love is penetration testing and you don't want to take the easy route, the Offensive Security Certified Professional (OSCP) course and certification has gained a well-earned reputation for toughness with a very hands-on learning structure and exam. The official online, self-paced $800 training course is called Penetration Testing with Kali Linux and includes 30 days of lab access. Because it relies on Kali Linux (the successor to pen testers' previous favorite Linux distro, BackTrack), participants need a basic understanding of how to use Linux, bash shells and scripts.

The OSCP is known for pushing its students and exam takers harder than other pen-testing paths. For example, the OSCP course teaches, and the exam requires, the ability to obtain, modify and use publicly obtained exploit code. For the "exam," the participant is given instructions to remotely attach to a virtual environment where they are expected to compromise multiple operating systems and devices within 24 hours and thoroughly document how they did it.

Offensive Security offers more advanced pen testing courses and exams including web, wireless, and advanced Windows exploitation. Readers might want to take advantage of their free, online basic Metasploit tool course.

Security+, CompTIA

CompTIA offers entry-level, comprehensive certification exams in PC repair (A+), networking (Network+), and security (Security+). Because a CompTIA exam is often the first test taken by many people new to the computer industry, it unfortunately has the reputation for being too basic a certification.

In my opinion, and by the standards of many employers, this is not true. The exams might not be as respected as other certification leaders, but they are comprehensive, and you must study hard to pass. CompTIA Security+ certification covers network security, cryptography, identity management, compliance, operation security, threats, and host security, among other topics. You get 90 minutes to complete 90 questions. I took the Security+ exam a long time ago, but it was tougher than expected for an exam that covers the basics. It even includes some simulated environments where the test taker has to select the right options. Price is $311.

Read the rest here:
https://www.csoonline.com/article/3116884/top-cyber-security-certifications-who-theyre-for-what-they-cost-and-which-you-need.html?nsdr=true

Quantum – a double-edged sword for cryptography

By Jon Cartwright, Homeland Security News Wire, June 14, 2019

Quantum computers pose a big threat to the security of modern communications, deciphering cryptographic codes that would take regular computers forever to crack. But drawing on the properties of quantum behavior could also provide a route to truly secure cryptography.

Defense, finance, social networking – communications everywhere rely on cryptographic security. Cryptography involves jumbling up messages according to a code, or key, that has too many combinations for even very powerful computers to try out.

But quantum computers have an advantage. Unlike regular computers, which process information in "bits" of definite ones and zeros, quantum computers process information in "qubits", the states of which remain uncertain until the final calculation.

The result is that a quantum computer can effectively try out many different keys in parallel. Cryptography that would be impenetrable to regular computers could take a quantum computer mere seconds to crack.

Practical quantum computers that can be used to break encryption are expected to be years, if not decades, away. But that should not be of any reassurance: even if a hacker cannot decipher confidential information now, they could save it and simply wait until a quantum computer is available.

"The problem already exists," said Professor Valerio Pruneri of the Institute of Photonic Sciences in Barcelona, Spain, and the coordinator of a quantum security project called CiViQ. "A hacker can take what is stored now, and break its key at a later date."

Read the rest here:

http://www.homelandsecuritynewswire.com/dr20190614-quantum-a-doubleedged-sword-for-cryptography

2019 Schedule of Events

Chapter Meetings – Dinner

Tuesday, July 16, 2019
Tuesday, August 20, 2019
Tuesday, October 15, 2019
Tuesday, November 19, 2019

Chapter Meetings – Lunch

Wednesday, July 17, 2019
Wednesday, August 21, 2019
Wednesday, October 16, 2019
Wednesday, November 20, 2019

Board Meeting

Tuesday, August 6, 2019

Mini-Seminars

Saturday, July 20, 2019
Saturday, August 24, 2019
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:

Women in Cybersecurity No Longer an 'Anomaly'

By Kacy Zurkus, Security Boulevard, June 12, 2019

Truth be told, there are many women in cybersecurity who are tired of talking about women in the industry as if they are anomalies. For many female professionals, it's far past the time for the narrative to change. Rather than be seen as a token representative of their sex, these cybersecurity professionals want to be (and in most cases are) respected for the quality of their work.

Indeed, it does seem that the pendulum is shifting. According to the numbers, women are holding more positions across all sectors of the cybersecurity industry at an ever-growing rate. In March, Cybersecurity Ventures predicted that women will represent more than 20% of the global cybersecurity workforce by the end of 2019, yet recent research from (ISC)2 reported that women already accounted for 24% of the cybersecurity workforce.

That number stayed stagnant at a mere 11% for the better part of the last decade. But, in the words of Bob Dylan, "The times, they are a changin'."

Arguably, it's becoming easier to find a surplus of women to write about in stories such as "100 Fascinating Women Fighting Cybercrime." These are the women who have, in large part, paved the way for today's young women—who, according to the (ISC)2 research, are young, educated and ready to take charge.

The Women in Cybersecurity report revealed that women in the industry are uniquely poised to reach leadership roles in higher percentages than their male counterparts. "Even though men outnumber women in cybersecurity by 3 to 1, more women are joining the field—and they are gunning for leadership positions," according to the report.

Redefining 'Women's Work'

Not only are women more highly educated than their male counterparts, but they also hold more certifications, according to the report.

"While 44% of men in cybersecurity hold a postgraduate degree, the number of women is 52%," the report noted. "By placing more emphasis on education and certification, women cybersecurity workers may be forging a path to career advancement and earning the qualifications to fill leadership roles. With this leadership comes more responsibility and credibility among peers, as well as a boost in salary."

In fact, the survey found that more women hold high-level management positions than do men, particularly in the roles of chief technology officer (7% women, 2% men), vice president of IT (9% women, 5% men) and C-level/executive (28% women, 19% men).

Still Room for Growth

While women and men tend to do the same work, they aren't equally compensated for their time and efforts. The report found that, on average, women in managerial positions are earning about $5,000 less than their male counterparts.

When asked about the types of tasks they are assigned, though, the duties of these men and women are nearly identical. The results of the survey yielded only a slight discrepancy in the number of male and female respondents who are responsible for security threat detection and remediation, data security, network security architecture, security consulting and securing cloud environments.

The challenges that cybersecurity teams face, whether comprised of men or women, are all too familiar: low security awareness among end users, inadequate funding, lack of highly skilled professionals and a lack of management support or awareness.

"In these areas, the gap between women and men is never that wide. For instance, the gap in the level of concern related to employers not listening to their input is only 2% (16% of women vs. 18% of men). And when it comes to concern over lack of work-life balance, again, the gap is a mere 2% (28% of women vs. 26% of men)," the report said.

Read the rest here:

https://securityboulevard.com/2019/06/women-in-cybersecurity-no-longer-an-anomaly/

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.

GAO Finds Critical Security Risks in 'Decades Old' Federal IT Systems

By Jon Cartwright, Homeland Security News Wire, June 14, 2019

The U.S. government plans to spend over $90 billion this fiscal year on information technology (IT). Most of that will be used to operate and maintain existing systems, including legacy systems which can be more costly to maintain and vulnerable to hackers.

A Government Accountability Office (GAO) report analyzed 65 federal legacy systems and identified the 10 most critical at 10 agencies. The systems were 8 to 51 years old.

Among the 10 most critical legacy systems that GAO identified as in need of modernization, several use outdated languages, have unsupported hardware and software, and are operating with known security vulnerabilities. For example, the selected legacy system at the Department of Education runs on Common Business Oriented Language (COBOL)—a programming language that has a dwindling number of people available with the skills needed to support it. In addition, the Department of the Interior's system contains obsolete hardware that is not supported by the manufacturers. Regarding cybersecurity, the Department of Homeland Security's system had a large number of reported vulnerabilities, of which 168 were considered high or critical risk to the network as of September 2018.

Of the 10 agencies responsible for these legacy systems, seven agencies (the Departments of Defense, Homeland Security, the Interior, the Treasury; as well as the Office of Personnel Management; Small Business Administration; and Social Security Administration) had documented plans for modernizing the systems. The Departments of Education, Health and Human Services, and Transportation did not have documented modernization plans. Of the seven agencies with plans, only the Departments of the Interior and Defense's modernization plans included the key elements identified in best practices (milestones, a description of the work necessary to complete the modernization, and a plan for the disposition of the legacy system). Until the other eight agencies establish complete modernization plans, GAO says they will have an increased risk of cost overruns, schedule delays, and project failure.

GAO therefore recommends the eight agencies identify and document modernization plans for their respective legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system. All agencies agreed with GAO's findings and are making plans to address the recommendation.

FEMA's System 4 vulnerabilities

The Department of Homeland Security (DHS)—Federal Emergency Management Agency's (FEMA) System 4 consists of routers, switches, firewalls, and other network appliances (all referred to as devices) to support the connectivity of FEMA sites. According to FEMA, System 4 needs to be modernized because there are significant cyber and network vulnerability risks associated with its end of life (i.e., no longer supported or manufactured by the vendor) devices. In particular, the system's devices typically require replacement every 3 to 5 years from the date of purchase. Despite this, the majority of the hardware was purchased between 8 and 11 years ago.

As of December 2018, about 545 of these devices were at the end of life. In a security assessment report performed in September 2018, System 4 received 249 security findings, of which 168 were high or critical risk to the system. Further compounding this issue, the agency is not certain exactly how many devices make up the system. In particular, FEMA officials stated that the vendor completed an inventory of devices in May 2018, but that inventory did not align with other inventory counts. As a result, the agency plans to develop an inventory reconciliation strategy and process to address this issue.

FEMA intends to replace System 4's devices in two phases. The first phase will target the agency's smaller facilities, while the second phase will address the larger facilities, which may require more complex installations. FEMA's Office of the Chief Information Officer is conducting site surveys to better define requirements and cost estimates. While the agency has yet to develop finalized modernization plans for this initiative with milestones, DHS officials and contract information technology staff developed a list of future recommended activities that would help modernize the system as part of their November 2018 quarterly business review.

Read the rest here:

https://www.hstoday.us/subject-matter-areas/information-technology/gao-finds-critical-security-risks-in-decades-old-federal-it-systems/

Bipartisan bill would enable companies to defend themselves against cyberattacks

By Maggie Miller, The Hill, June 13, 2018

A bipartisan pair of lawmakers is seeking to enable companies to defend themselves in cyberspace.

The Active Cyber Defense Certainty Act, introduced Thursday by Reps. Tom Graves (R-Ga.) and Josh Gottheimer (D-N.J.), would allow companies and individuals to leave their own networks and defend against malicious actors seeking to attack them.

The bill would allow authorized individuals and companies to go onto other networks in order to establish who is attacking them online, to disrupt a cyberattack as it is occurring, to retrieve or destroy stolen files, to utilize beaconing technology and to monitor the behavior of the malicious actor.

"Technology has outpaced public policy, and our laws need to catch up," Graves said in a statement. "We must continue working toward the day when it's the norm – not the exception – for criminal hackers to be identified and held accountable for their crimes."

The legislation would also require these individuals and companies to notify the FBI's National Cyber Investigative Joint Task Force and receive a response before being allowed to take any of the defense steps.

The measures in the bill would involve updating the Computer Fraud and Abuse Act (CFAA), with Graves's office describing these changes as constituting "the most significant update to the CFAA since its enactment." This law was enacted in 1984, and limits unauthorized access to computer systems.

Read the rest here:

https://thehill.com/policy/cybersecurity/448476-bipartisan-bill-would-enable-companies-to-defend-themselves-against

FBI warns users to be wary of phishing sites abusing HTTPS

By John E. Dunn, Naked Security, June 12, 2019

Would you trust a website simply because the connection to it is secured using HTTPS backed by the green padlock symbol?

Not if you're informed enough to understand what HTTPS signifies (an encrypted, secure connection with a server) and doesn't signify (that the server is therefore legitimate).

This week the FBI issued a warning that too many web users view the padlock symbol and the 'S' on the end of HTTP as a tacit guarantee that a site is trustworthy.

Given how easy it is to get hold of a valid TLS certificate for nothing, as well as the possibility that a legitimate site has been hijacked, this assumption has become increasingly dangerous.

Unfortunately, cybercriminals have spotted the confusion about HTTPS, which accounts for the growing number of phishing attacks deploying it to catch people off guard. The FBI alert confirms:

> *They [phishing attackers] are more frequently incorporating website certificates – third-party verification that a site is secure – when they send potential victims emails that imitate trustworthy companies or email contacts.*

How we got here

Today, all competently managed websites use HTTPS, a big change from even a handful of years ago when its use was limited overwhelmingly to sites either allowing password login or conducting transactions as required by the industry PCI-DSS card standard.

What supercharged the use of SSL/TLS certificates and HTTPS was Google's insistence from 2015 that its presence would become a positive signal for its search engine algorithms.

Read the rest here:

https://nakedsecurity.sophos.com/2019/06/12/fbi-warns-users-to-be-wary-of-phishing-sites-abusing-https/

How much risk small businesses really pose to supply chain cybersecurity?

By Staff, HelpNetSecurity, June 25, 2018

50% of large enterprises view third-party partners of any size as a cybersecurity risk, but only 14% have experienced a breach as the result of a small business partner, while 17% have been breached as the result of working with a larger partner, according to ISC2.

The study surveyed more than 700 respondents at both small businesses and large enterprises to learn how data sharing risk is perceived.

These findings contradict the widely-held belief that small businesses serve as the easiest conduit for cyberattacks on large enterprises.

The reality is that large enterprises are nearly unanimously confident (94% of survey respondents indicated that they are "confident" or "very confident") in their small business partners' cybersecurity practices, and 95% have a standard process for vetting their suppliers' cybersecurity capabilities.

"This research highlights the fact that building a strong cybersecurity culture and subscribing to the right best practices can help organizations of any size maximize their security effectiveness," said ISC2 COO Wesley Simpson.

"It's a good reminder that in any partner ecosystem, the responsibility for protecting systems and data needs to be a collaborative effort, and multiple fail safes should be deployed to maintain a vigilant and secure environment. The blame game is a poor deterrent to cyberattacks."

Lax access management controls

Nearly two-thirds (64%) of large enterprises outsource at least one-quarter (26%) of their daily business tasks, which requires them to allow third-party access to their data. These outsourced functions can include anything from research and development, to IT services and accounts payable.

This data access and sharing is necessary as a large enterprise scales its operations, but the ISC2 research indicates that access management and vulnerability mitigation is often overlooked.

- 34% of large enterprises say they have been surprised by the broad level of access a third-party provider has been granted to their network and data
- 39% of small businesses expressed the same surprise about the access they were granted when providing services to large enterprise partners
- Even worse, 35% of large enterprises also admitted that when alerted by a third party to insecure data access policies, nothing changes in the large enterprise's practices
- More than half (55%) of small business respondents reported that they still had access to a client's network or data after completing a project or contract

54% of small businesses have been surprised by some of their large enterprise clients' inadequate security practices, and 53% have provided notification of security vulnerabilities they've discovered in large enterprise networks to which they have access

Investment in cybersecurity teams

The report also found that while small businesses have fewer employees overall, the proportion of their cybersecurity staff isn't necessarily lower than in large enterprises. The study shows that nearly half (42%) of small businesses, with 250 or fewer workers, employ at least five dedicated cybersecurity staff.

Read the rest here:

https://www.helpnetsecurity.com/2019/06/25/risk-small-businesses/

IG: DHS needs more election tech help, IT patching

By Mark Rockwell, FCW, May 31, 2019

The Department of Homeland Security could use a few more hands to help it tackle cybersecurity issues ranging from election security efforts to simple security procedures for its internal networks, the agency's inspector general told Congress in a new report.

"Additional staff could enhance DHS' ability to provide technical assistance and outreach to state and local election officials during elections" moving forward, the DHS Office of Inspector General said in its semiannual congressional report released on May 31 that summed up its oversight activities between October 2018 and March 2019.

The report also noted DHS also still needs to improve its patch management process and take action to protect the personal data of disaster survivors.

The OIG cited a February report that said the agency's efforts to help state and local governments secure their election infrastructure with mitigation and threat detection services had been hindered by shifting agency leadership, administrative staff shortages and a lack of metrics. DHS responded that its new Cybersecurity and Infrastructure Security Agency was working to remedy those gaps, including prioritizing hiring operational and administrative staff, as well as increasing its outreach to state and local governments.

There was good news and bad news for the agency on its Federal Information Security Modernization Act efforts to secure sensitive data. The OIG said although DHS had been effective in protecting its most secret systems in 2018, reaching "Level 4 – Managed and Measurable" in three of five cybersecurity functions, it still had basic issues with timely patch management.

DHS also told the IG it was working to close data security gaps in its Transitional Sheltering Program for disaster survivors' short-term housing needs. In March, the OIG reported that DHS had improperly released sensitive personal data on 2.3 million survivors of hurricanes Harvey, Irma, and Maria and the California wildfires.

Read the rest here:

https://fcw.com/articles/2019/05/31/dhs-ig-roundup-rockwell.aspx?admgarea=TC_Security

Census' Cybersecurity Plan is Full of Holes, Watchdog Says

By Jack Corrigan, NextGoc, June 3, 2019

Federal auditors uncovered numerous holes in the Census Bureau's plans for combating the significant cybersecurity and tech threats facing the 2020 count, which could leave officials struggling to respond to disruptions.

The Government Accountability Office found the bureau's plan for mitigating cybersecurity risks during the 2020 Census left out many of the defensive tactics officials previously said they would use to defend IT systems from attack. For example, the initial plan included no information about how the bureau would gather threat intelligence from other federal agencies, something officials had long said they planned to do, auditors said in a reportpublished Friday.

After GAO pointed out the omission, Census officials updated the plan to include threat sharing activities, but it remains "just one of several [cybersecurity] services" other agencies are expected to perform on the bureau's behalf, auditors said.

"If the bureau's plan for mitigating cybersecurity risks to the census omits such key activities, then the bureau is limited in its ability to track and assess those activities, and to hold individuals accountable for completing activities that could help manage cybersecurity risks," they wrote.

While most of the attention on the 2020 Census has focused largely on the Trump administration's controversial citizenship question, GAO officials and others have for yearswarned that tech and cyber issues could be one of the biggest obstacles to an accurate count. The upcoming decennial will mark the first time residents can submit responses over the internet, which makes it particularly susceptible to online attacks and misinformation.

The bureau fell far behind schedule on rolling out the various IT systems needed to conduct the decennial, and in the most recent report, auditors confirmed there remains lots of work to be done ahead of the 2020 count. As of February, the bureau was still in the process of developing 39 of the 52 IT systems needed for the decennial, and 43 of the systems still hadn't fully completed testing, GAO said.

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/06/census-cybersecurity-plan-full-holes-watchdog-says/157444/

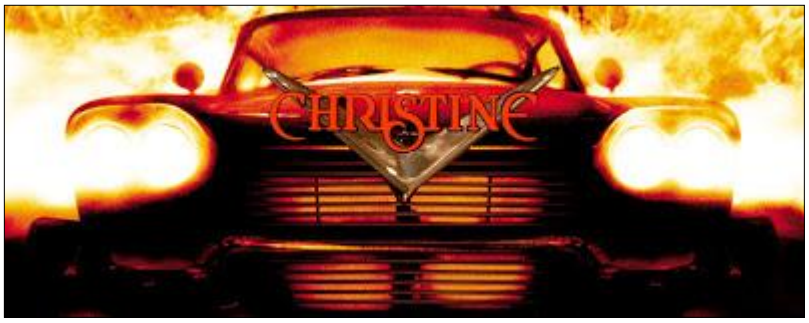
How likely are weaponized cars?

By Matan Scharf HelpNetSecurity, June 3, 2019

It is easy to become absorbed by the exaggerated Hollywood depictions of car hacking scenarios – to imagine a not-so-distant future when cars or their supporting infrastructures are hacked by criminals or terrorists and turned into lethal weapons. There are reasons why such a scenario has not happened yet. But could it? And if so, how can we prevent it?

Some might argue that the likelihood of cars being weaponized is extremely low, but from a purely technical standpoint, there is nothing stopping attackers who invest the time and effort from achieving such a feat. After all, the most fundamental property of a computer system is the software that governs the operation of the device. Software is inherently susceptible to a wide variety of threats and vulnerabilities. Under the appropriate conditions, any system may be compromised and its behavior altered, leading to undesired consequences.

How does that affect vehicles?



Technological advancements of the last 20 years or so have led to a dramatic change in the core definition of what a vehicle is. Traditionally, a vehicle was understood to be an isolated mechanical machine, powered by fossil fuel, and driven by a human. This definition is evolving as automotive technology evolves.

The modern vehicle can be described as electric, connected, software embedded, driverless, and even artificially intelligent. Left unmanaged and without security considerations, these properties render risks that manifest as software bugs and design flaws that may allow unauthorized remote access. As vehicles become ever more connected and as software spreads into more and more safety-critical systems, these bugs and flaws present an opening for a catastrophic failure, which may result in injury or even loss of life.

Up to this point in the discussion, we've only explored the threats to a single vehicle. When we look at this threat at scale, we're talking about how smart, connected, autonomous cars could be the 21st century's weapon of mass destruction. Just imagine fleets of remotely controlled—or even worse, autonomous—vehicles slamming into everything in their path.

The automotive industry is not oblivious to these risks—far from it. And regulatory bodies have drafted legislation, standards, and compliance requirements designed to prevent such catastrophic failures. But as history has shown us, time and time again, even when rigid and compulsory compliance requirements such as HIPAA (medical), PCI (finance), and ISO are enforced, they aren't enough to prevent some of the most notorious breaches and data leaks.

We need to acknowledge that there is an underlying force at work here. As humans are inherently exposed to health hazards, the automotive industry is susceptible to software quality issues that lead to cybersecurity threats.

Let's now take this examination one step further and look into the DNA of automotive companies to articulate the challenge at its core: the reality of vehicle production.

Order of magnitude disruption

Historically, automakers were experts in designing and managing the production of vehicles in high volumes under strict quality and safety requirements. In this case, "quality" was mostly a question of luxury, performance, and ride comfort, and "safety" was defined and measured as a derivative of collision tests, fault tolerance, and other attributes reflecting the vehicle's ability to protect the driver, passengers, and surrounding pedestrians from injury in an accident. This paradigm was embedded deeply into the design, production, and manufacturing processes of vehicles.

Along came cyber

But then everything changed. This change didn't happen overnight. It wasn't announced ahead of time so that the industry could plan accordingly. Instead, over two decades, vehicles gradually became specific attack targets.

"Safety" has become a derivative of secure software development life cycle (SSDLC) practices, and "quality" has become the ability to enforce software quality downstream in the software supply chain.

Read the rest here:

https://www.helpnetsecurity.com/2019/06/03/weaponized-cars/

NIST's Real Impact on Innovation and Quality of Life

By Laura Ost, NIST, June 18, 2019

Measurements are key to scientific and technological innovation. It's like a field of dreams: Better measurements always find useful applications.

Proving this credo, NIST's nearly 120 years of research to advance measurement science, standards and technology have had significant impacts on American innovation and quality of life.

This is remarkable for a small federal agency focused on developing practical solutions to the nation's ever-changing technology needs.

"NIST has the broadest science and technology portfolio of any science agency in the United States and likely in the world," says Walter G. Copan, under secretary of commerce for standards and technology and NIST director.

Since becoming director of NIST in 2017, Copan has been impressed by the widespread respect for and trust in NIST, as evidenced at a July 2018 media-sponsored event attended by representatives of industry and the U.S. Congress.

"Every one of them walked up to me and said, 'We love NIST,'" Copan says. "NIST provides tremendous value to the nation."

One senator reported walking along the Florida seashore and seeing buildings that had collapsed during a hurricane, located side by side with others still standing — standing because they were built to comply with NIST-recommended codes and standards.

What is the true value of something like that? Measurement advances can have a human impact that goes beyond numbers.

Copan notes that NIST has a history of generously "giving things away," and as a result is not always recognized as the source of an innovation. He aims to fix that through an ambitious effort that will make it easier for even more NIST innovations to make it out into the real world and for the country to get a bigger return on all federal investment in research and development.

Valuing the Invaluable.

NIST's impacts are often so broad or deep that they can't be fully measured. Some NIST technologies are used by most Americans, may form the basis for new products or even industries, and can even save lives. Although there is no comprehensive dataset of NIST's impacts, history offers many examples. Below are a few highlights.

NIST was a leader in the early days of radio, pioneering, among other things, the instrument (or blind) landing system. Anyone who has flown on an airplane at night or in cloudy weather, when the pilot can't see much, can thank NIST for this system. Blind landing relying on radio guidance also provides the basis for today's air traffic control systems.

NIST has long maintained U.S. civilian time standards, which support everyone who keeps a schedule, uses a phone or electricity, or owns stocks. NIST's Internet Time Service responds to about 40 billion automated requests per day to synchronize clocks in computers and network devices, while NIST radio broadcasts update an estimated 50 million watches and other clocks daily. NIST official time supports the time-stamping of hundreds of billions of dollars in U.S. financial transactions each working day.

Another pervasive NIST technology is closed captioning. Originally called TvTime, a method for broadcasting time and frequency data on television, this Emmy Award-winning technology has greatly benefited the deaf and hard of hearing. It is widely used on television and cable programs as well as motion pictures and has spawned an industry of suppliers of closed captioning services.

NIST benefits public health and safety in many ways. NIST engineering studies of fires and structural failures have led to significant changes in practices, standards and codes to enhance the health and safety of the publ

Read the rest here:

https://www.nist.gov/featured-stories/nists-real-impact-innovation-and-quality-life

Information Systems Security Association
Developing and Connecting Cybersecurity Leaders Globally
Colorado Springs Chapter

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: Mark Maluschka
- 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: **Vacant**
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

Can smart home devices get viruses? Experts separate fact from fiction

By Ben Lovejoy, 9TO5Mac, June 27, 2019

Can smart home devices get viruses? There's been a lot of talk about the idea of IoT (Internet of Things) devices being infected by viruses, not least because Samsung this month recommended scanning its QLED televisions for viruses every few weeks.

Read the rest here:

https://9to5mac.com/2019/06/27/can-smart-home-devices-get-viruses/

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