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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 10 OCTOBER 2020

Autumn Has Arrived

A Note From Our President

By Mr. Ernest Campos

Autumn is now upon us. Welcome to cooler temperatures, colorful foliage, and all things pumpkin spice. What a beautiful time of the year! As our chapter heads into Fall, we find ourselves busy with lots of internal and external projects at hand. In this month's article, I will do my best to catch you up on everything taking place. There is a lot to cover so, …. Hang on!

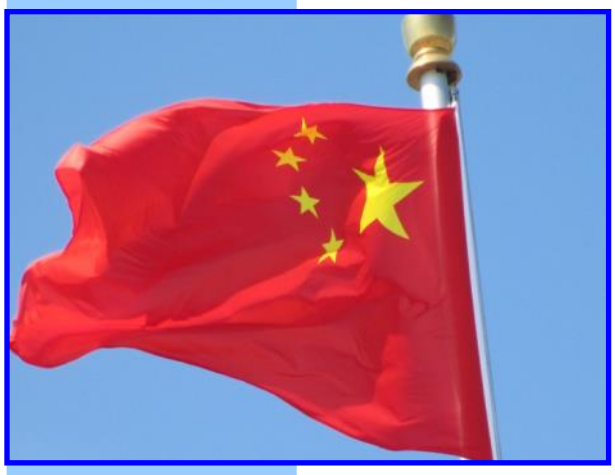
ISSA-COS Online Series – With the onset of COVID-19 back in March 2020, all in-person events were immediately halted. Many chapters throughout ISSA International were forced to suspend operations and even to this day, have not yet resumed activities. Fortunately, our chapter was able to quickly shift gears as we instituted virtual events; the first ever in the history of our chapter. This allowed us to keep presenting applicable content, sustain knowledge sharing, and continue to make the ability to earn CPE/CEU credits available to our members. Over the last seven months, nearly 800 participants have registered to attend our chapter's online presentations. We have featured nearly 40 guest speakers and have issued over 1000 CPE/CEU credits. Numerous industry businesses and organizations soon took notice of our chapter's events. As a result, sponsorships and strategic partnerships increased. The ability to become flexible during adverse times has enabled our chapter to not only remain open but, to thrive! As or the virtual presentations, what was initially designed to be a convenient alternative to meeting in-person has quickly become a core necessity. In addition to eventually resuming in-person events, our board of directors recently agreed to retain virtual events as a part of our permanent programming. Hooray!!

Cybersecurity Awareness Month – Each year, the month of October is Cybersecurity Awareness Month. Each year, to help increase emphasis on Cybersecurity, our chapter hosts a community panel discussion. During this event, we invite various Cybersecurity leaders from across our region to discuss with us their thoughts and observations regarding any number of Cyber-related topics. This year, this event will be held virtually on Thursday, October 22nd from 6 – 7:30 PM. The theme for this event is "*Adjusting to a Virtual Lifestyle: Impacts and Predictions on Work, Commerce, and Education*." ISSA-

(Continued on page 4)

Chinese database details 2.4 million influential people, their kids, addresses, and how to press their buttons

By Simon Sharwood, The Register, September 15, 2020



A US academic has revealed the existence of 2.4-million-person database he says was compiled by a Chinese company known to supply intelligence, military, and security agencies. The researcher alleges the purpose of the database is enabling influence operations to be conducted against prominent and influential people outside China.

"...what cannot be underestimated is the breadth and depth of the Chinese surveillance state and its extension around the world."

The academic is Chris Balding, an associate professor at the Fulbright University Vietnam.

And he says the company is company is named "Shenzhen Zhenhua".

Security researcher Robert Potter and Balding co-authored a paper claiming the trove is known as the "Overseas Key Information Database" (OKIDB) and that while most of it could have been scraped from social media or other publicly-accessible sources, 10 to 20 per cent of it appears not to have come from any public source of information. The co-authors do not rule out hacking as the source of that data, but also say they can find no evidence of such activity.

"A fundamental purpose appears to be information warfare," the pair stated.

Balding wrote on his blog that the database contains the following:

The information specifically targets influential individuals and institutions across a variety of industries. From politics to organized crime or technology and academia just to name a few, the database flows from sectors the Chinese state and linked enterprises are known to target.

The breadth of data is also staggering. It compiles information on everyone from key public individuals to low level individuals in an institution to better monitor and understand how to exert influence when needed.

The database includes details of politicians, diplomats, activists, academics, media figures, entrepreneurs, military officers and government employees. Subjects' close relatives are also listed, along with contact details and affiliations with political and other organisations.

In the paper, the pair said all that data allows Chinese analysts "to track key influencers and how news and opinion moves through social media platforms."

"The data collected about individuals and institutions and the overlaid analytic tools from social media platforms provide China enormous benefit in opinion formation, targeting, and messaging."

It gets worse: "From the assembled data, it is also possible for China even in individualized meetings be able to craft messaging or target the individuals they deem necessary to target."

Balding said the database is "technically complex using very advanced language, targeting, and classification tools."

But it was also hard to investigate, as parts were reportedly corrupt.

Balding therefore shared the data trove with Potter - of Australian security firm Internet 2.0 - to help make it accessible. The results were shared with select, non-*Reg* media outlets.

The Register has sought comment from Balding and Internet 2.0 but had not received a reply at the time of writing.

Read the rest here:

https://www.theregister.com/2020/09/15/china_shenzhen_zhenhua_database/

Membership Corner

Membership Update

Have you updated your contact information on the ISSA International website? You have! That is awesome. If you have not, please log onto the ISSA International website and click on your welcome icon on the top of the page and select “Account + Settings”. Once there you can make your updates. Thank you for your support.

We need all members to spread the word that we are looking for new members to join our great organization. Below are the top 10 reasons join ISSA!

Top 10 Reasons Cybersecurity Professionals Join ISSA

1. Build professional relationships
2. Keep up on developments in information security/risk/privacy
3. Content of chapter meetings
4. Professional development or educational programming offerings
5. Earn CPEs/CPUs
6. Learn practical/best practices solutions
7. Career information and employment opportunities
8. Advance the profession
9. Give back to the profession
10. Develop the next generation of cybersecurity professionals

New Members September
None

Our membership is hanging in at ~337 members as of the end of September 2020.

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

Thanks,

Steven Mulig

Vice President of Membership

membership@issa-cos.org

Join ISSA!

Membership applications are administered through the ISSA International website. The process is quick and easy… just 5 simple steps! Once registered, remember to stay up to date with ISSA-COS chapter events by regularly visiting the **www.issa-cos.org** website. Here is how you can join today!

1. Go to **www.issa.org**
2. Click on "**JOIN**"
3. Select a **Membership Type**
4. Select "**Colorado Springs**" as your **Home Chapter**
5. Complete the **Membership Form** and **Payment Process**

For more information about membership, email:
membership@issa-cos.org

(Continued from page 1)

COS is honored to announce Ms. Vanessa Johnson, President of AFCEA-RMC, will serve as our moderator for this event. Among our other invited participants, we are also honored to announce Mr. Thomas Russell, NCC Director of Education, will be participating. To attend this event, please register via our website at www.issa-cos.org.

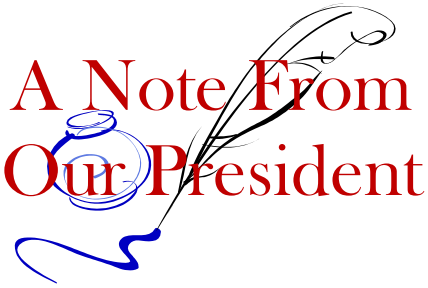
10th Annual Peak Cyber Symposium – PCS is right around the corner! Since the decision to move this event to a virtual platform, everything about this event just keeps getting bigger! The duration of PCS will now span 4-days! The number of exhibitors continues to grow! The number of community partners continues to grow! The number of nation-wide registrants continues to grow! Everything about this event is getting bigger and bigger. Even the number of keynote speakers continues to grow! Our list of keynote speakers now includes:

- Dr. Jim Crowder – Systems Fellow, Mad Scientist Colorado Engineering, Inc.
- Dr. Rory Lewis – Program Director: MS of CS, UCCS; Director: AI USAF/A2 Wedge SOCOM
- Dr. Dale Meyerrose – USAF MG (Ret); President, MeyerRose Group
- Dr. Kelley Misata – CEO Sightline Security; President and Exe Director, OISF (Suricata)
- Mr. Nathan Toups – Sr. Site Reliabilty Engineer, Sante Capital Quantitative Hedge Fund
- Ms. Karen Worstell – CEO, "W" Risk Group
- Dr. Ron Ross – Fellow, NIST; Principal Author of NIST SP 800-53 Rev 5 ** **Just Confirmed** **

What an exciting event this symposium is shaping up to become. If you have not yet registered, please do so at www.peakcyberco.com. Remember, this event is **FREE** for all ISSA members (regardless of chapter affiliation), and anyone with a (dot) mil, (dot) gov, or (dot) edu email address.

ISSA-COS Annual Elections – Once again, election season is upon us! ISSA-COS is now announcing our "Call for Candidates." Anyone interested in running for an open position is welcome to register as a candidate by contacting our Annual Election Committee at past-president@issa-cos.org. Candidates must be General Members of ISSA-COS and members in good standing (i.e., no ethics violations and currently paid dues). Newly elected candidates will be expected to attend and observe the December 2020 Board Meeting in preparation for the assumption of their roles January 1, 2021. This year, the positions up for election include the following:

- President and Chair(person) of the Board
- Vice President of Training
- Director of Certification
- Recorder/Historian
- Director of Professional Outreach
- Member-at-Large #3
- Member-at-Large #4



Updated Chapter Bylaws – As a part of the 2020 Annual Election, General Members will be asked to vote on the institution of newly updated bylaws for our chapter. For several months, volunteer board members and key personnel have poured countless hours into the task of updating our chapter's governing documents. The newly revised documents have been drafted with an emphasis on increased flexibility in governance for the future needs of our chapter. General Members will be invited to review the bylaws as a part of this year's voting process. Look for special announcements to be sent via email later this month.

Indeed, quite a bit is happening with our chapter. I am proud ISSA-COS has been able to continue operations this year and as well look forward to 2021, we are well position to expect another great year of activities. As always, I thank our **volunteers** who help keep or chapter running strong. I also thank our principal sponsors (**Murray Security Services, Jacobs, and Beyond Trust**) for their financial support. I thank our **Community Partners** who support our events throughout the year. Most of all however, I thank our **General Members** who help make ISSA-COS a pillar institution within our community!

Sincerely,

Ernest

Who's on Your Side?

By Colleen Murphy, ISSA-COS, September 26, 2020

The healthcare sector has been under tremendous pressure with the increase in the number of those afflicted due to the COVID-19 pandemic and cybercriminals have left no stone unturned to take advantage of this situation.

For cybersecurity professionals, users are often referred to as "the weakest link" in an organization's security posture. And some of us may have used the phrase "ID-TEN-T" at one time or another to describe a user. The term "weakest link" is defined as "the least strong or successful part". Taken in context by cybersecurity professionals, this means we consider people to be the weakest part of the people-process-technology triad. But people can also be one of your biggest strengths – and early warning system – for attacks. We're all human and humans make mistakes, including the most dedicated, conscientious employees. The Occupational Safety and Health (OSH) Wiki (https://oshwiki.eu/wiki/Human_error) points out that stress can increase the probability of errors, and that "It is generally accepted that 80-90% of accidents are due to human error". And who isn't under stress these days?

In addition to daily stress, hackers do their best to trick users into making mistakes. Some users, unfortunately, are more likely to click on "bad" links than others. Per the 2018 Verizon Data Breach Investigative Report, page 11, "the more phishing emails someone has clicked, the more they are likely to click in the future." While the majority of users won't fall for phishing emails, the hacker only needs one user to click to succeed. And, "an average 4% of people in any given phishing campaign will click it" (Verizon 2018 DBIR, page 12). Anyone of us, at any time, may fall victim to a phishing email. Even the best of us, if you're stressed, tired, distracted, overworked, or rushed, you can fall for a phishing attack. From the most junior employee to the company CEO, it may just be a matter of time before you are tricked by a sophisticated phishing email.

If the reality means phishing attacks will succeed, shouldn't we focus our attention on leveraging users as an early warning system? Since most users will detect – and not click – on phishing emails, they can be your best source of awareness that an attack is occurring. Unfortunately, 83% don't report phishing attacks (Verizon 2018 DBIR, page 13) when they see one. How do we change their attitude? How do we get a greater percentage of the 83% who detect a phishing attack to report it? If you don't know there's a phishing attack out there, how do you respond to it? If users aren't reporting phishing attacks, how do you get them to?

The relationship between cybersecurity professionals and users is perhaps similar to the relationship between management and employees in general. As such, we may be able to leverage proven methods to engage employees in the workplace in a similar manner to better engage users in the cybersecurity realm.

The following are a few suggestions to get users to engage more with IT/cybersecurity personnel to the benefit of the entire organization.

1. Appreciate your users. Acknowledge the challenges users may be facing every day. Understand their role in the company. Stop referring to them as the "weakest link". Encourage users to be part of your extended cybersecurity team.

2. Be transparent. Provide the "why" for security controls. Help users understand the need to report phishing emails – and other cybersecurity-related issues. Make them part of the extended team, part of the solution. Give them a sense of engagement in protecting the company's IT resources. Create a team environment, encourage compliance with company policy and guidance.

3. Be visible. When/where possible, get out from behind the keyboard and engage users. Be accessible so that users see you as approachable and available for guidance and assistance, rather than the inspector or enforcer. Acknowledge users for their help and support.

4. Be known. Users are people, not "userids". Relationships between cybersecurity professionals and users can build cooperation and teamwork.

5. Be flexible. When possible, give users options to meet their needs while still meeting cybersecurity requirements.

Per the 2020 Verizon DBIR, page 50: "It is exceedingly important to encourage your user base to let you know when your organization is being targeted. If they don't report it, you miss out on your early warning system."

Yes, users can cause problems. But they can also help. Don't miss the opportunity to leverage users to help keep your network secure. Make them part of your extended team – get them on your side.

PEAK CYBER
10th ANNUAL SYMPOSIUM

To the 10th Annual Peak Cyber Symposium Attendees

Thank you for registering to for Peak Cyber!

I hope you are doing well during these challenging times. We are contacting you because

ISSA-COS has decided to take the 10th Annual Peak Cyber Symposium **virtual** this year. Given the current COVID-19 situation, and new guidelines for attendee capacity at the Doubletree Hilton, it became clear that there was really no other choice but to go **virtual.**

Because we are pivoting to a virtual program we need a little more time to get things in order so we are also pushing the event dates out to November The new schedule will be:

- Monday, **November 16th** – Peak Cyber Job Fair
- Tuesday, **November 17th** – Peak Cyber CTF
- Wednesday, **November 18th** – Peak Cyber Speaker Sessions and Virtual Exhibits
- Thursday, **November 19th** – Peak Cyber Speaker Sessions and Virtual Exhibits

Detailed instructions will be emailed out to you on how to access Peak Cyber via the Whova Event App as the event approaches.

In the meantime, help us spread the word to your co-workers and colleagues. The virtual event will remain ***FREE to attend for all ISSA Members and those with a mil, .gov, or .edu email address.***

COVID-19 has created an extremely challenging business environment, and in the conference industry, it has been even more challenging. We appreciate your understanding and support.

Please feel free to contact me with questions or concerns.

Respectfully,

Dennis O'Neill

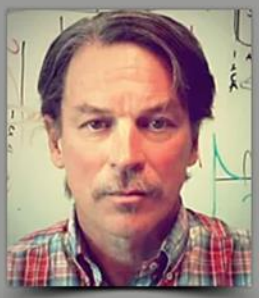
ISSA-COS Peak Cyber Lead

dennis@ssewest.com

Peak Cyber Symposium

KEYNOTE SPEAKERS

Dr. Jim Crowder
Systems Fellow,
Mad Scientist
Colorado Engineering, Inc.



Dr. Rory Lewis
Program Director: Masters of Computer Science, UCCS |
Director: Artificial Intelligence
USAF/A2 WEdge SOCOM

JUST CONFIRMED!

Dr. Dale W. Meyerrose
Major General, U.S. Air Force retired
President, MeyerRose Group

JUST CONFIRMED!

Dr. Kelley Misata
CEO
Sightline Security |
President and Executive Director
OISF (Suricata)

Nathan Toups
Senior Site Reliability Engineer
Santé Capital
Quantitative Hedge Fund

JUST CONFIRMED!

Karen Worstell
CEO
W Risk Group

Early Bird Registration is now open.

***Free registration* for all ISSA Members, .mil, .gov. and .edu!**

www.peakcyberco.com

How the government is keeping hackers from disrupting coronavirus vaccine research

By Shannon Vavra, CyberScoop, September 8, 2020

Six months ago, as professional sports were postponed indefinitely, schools were shuttering, Tom Hanks was the poster boy for COVID-19, and President Donald Trump addressed a nervous nation, people at the highest levels of the U.S. government became laser-focused on one idea: Coronavirus vaccine research needed to be defended from hacking attempts.

Soon after the World Health Organization declared a pandemic, the Pentagon's Defense Digital Service and the National Security Agency got to work on a behind-the-scenes protection mission for "Operation Warp Speed," the U.S. government program responsible for producing 300 million coronavirus vaccine doses by January 2021.

Known as the Security and Assurance portion of Operation Warp Speed, the mission is no small effort. Consisting of people from DDS, NSA, FBI, the Department of Homeland Security and the Department of Health and Human Services, it has been running behind the scenes for months, and is being detailed here for the first time.

The effort's main goal is to provide cybersecurity advice, guidance, and services to pharmaceutical giants developing a vaccine or working on manufacturing and distribution, as well as government agencies participating in OWS, multiple U.S. government officials involved in the operation told CyberScoop. The companies involved are pillars of the industry: Johnson & Johnson, AstraZeneca, and Moderna are among those working on the medicine, while companies like Emergent BioSolutions, SiO2, and Corning will be responsible for dispersing that medicine to people. The companies, in addition to the government agencies working on OWS, are highly visible and vulnerable organizations.

The task is one of the most sweeping, high-profile cybersecurity supply chain issues the U.S. government has ever attempted to solve. The damage that could be wrought from a cybersecurity incident goes beyond a massive loss of intelligence or money: It could cost lives.

The pandemic has been a clarion call to supply chain security efforts for the entire federal government, according to Bill Evanina, the Director of the National Counterintelligence and Security Center at the Office of the Director of National Intelligence.

"COVID has really awoken not only the federal government, but a lot of people, with respect to supply chain," said Evanina, who was speaking broadly about hackers targeting U.S. coronavirus response efforts at a U.S. Chamber of Commerce event in July. "Once we identify a vaccine, we have to manufacture that and distribute that. That provides a lot of vulnerabilities for adversaries to infiltrate the supply chain. We have to be able to secure that."

Read the rest here:

https://www.cyberscoop.com/operation-warp-speed-coronavirus-vaccine-cybersecurity-dds-nsa-dhs-cisa-fbi-hhs/

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.

Join ISSA-COS on Social Media

Twitter:

- Colorado Springs ISSA
- @COSISSA

LinkedIn:

- ISSA Colorado Springs Chapter
- https://www.linkedin.com/groups/1878203/

Facebook:

- Colorado Springs Chapter of the ISSA
- @ColoradoSpringsISSA

Upcoming Online Series Events

10/22/2020 – National Cybersecurity Awareness Month!

Speaker: Ms. Vanessa Johnson, AFCEA-RMC

Panel Discussion: Colorado Springs Community Partners

Topic: *Adjusting to a Virtual Lifestyle: Impacts and Predictions on Work, Commerce, and Education*

11/05/2020

Speaker: Mr. Michael Wylie, *Director of Cybersecurity Services, Richey May Technology Solutions*

Topic: *Encore Presentation Part 2, "Intro to Malware Analysis & Response"*

12/03/2020

Speaker: TBD

Register at: *www.issa-cos.org*

To become a guest speaker,
e-mail us at:
SpeakersBureau@issa-cos.org

ISSA-COS 2020 Elections

Call for Candidates:

ISSA-COS is now accepting candidates for the following positions:

- **President and Chair(person) of the Board**
- **Vice President of Training**
- **Director of Certification**
- **Recorder/Historian**
- **Director of Professional Outreach**
- **Member-at-Large #3**
- **Member-at-Large #4**

Candidates must be General Members of ISSA-COS and members in good standing (i.e., no ethics violations and currently paid dues).

To register as a candidate, email:
past-president@issa-cos.org

SPECIAL INTEREST GROUPS (SIGS)

SIG Overview

The ISSA-COS Special Interest Groups (SIGs) are comprised of Cybersecurity professionals who gather to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: **Affinity Groups** and **Industry Groups**. Through our online forum, ISSA-COS enables our members and the community at large to participant in thoughtfully organized and well-structured categories of conversation. Forum participants can engage in any one of eight different SIGs. Within our forum, we commission Subject Matter Experts who add increased technical knowledge to all the conversational threads.

To maintain positive behaviors within the forum, ISSA-COS has assigned a SIG Program Coordinator who monitors each SIG conversation. The SIG Program Coordinator also monitors the size and degree of participation within each SIG. Once participation reaches a sizable amount, the SIG Program Coordinator will suggest and help organize in-person meet ups. This provides SIG participants an opportunity to put virtual names with physical faces to further strengthen the bonds of interaction taking place in the virtual environment.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups 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 (WIS)
- Young Professional in Security (YIS)
- Educators in Security (EduIS)
- Executives in Security (ExecIS)

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups 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 (FIS)
- Healthcare in Security (HIS)
- Retail in Security (RIS)
- DoD in Security (DodIS)

Instructions & Credit for Online Playbacks of ISSA-COS Training Sessions

- Video playbacks are available to ISSA-COS members within 3-days
- Navigate to the www.issa-cos.org website
- Login using your *COS Chapter* credentials
- Navigate to "Training" and select the desired month
- Select the desired presentation and enjoy the playback
- Upon completion of the playback, email: certification@issa-cos.org and identify the *month* and *session number* for the episode you viewed

Cyber Attack Most Likely Space Threat: Maj. Gen. Whiting

By Theresa Hitchens, Breaking Defense, September 16, 2020

Cyber defense is a top mission priority for the Space Force, says Maj. Gen. Stephen Whiting, deputy commander of the new service.

"We know that cyber attack is where we are most likely to face the enemy in space," Whiting said, if for no other reason than the barriers to entry for cyber attack capabilities are lower than for other forms of satellite attack.

Therefore, he told the annual AMOS space conference in Hawaii today, cyber defense "will be a principal focus area of the United States Space Force as we move forward."

Further, Whiting explained, Space Force has decided the centrality of the mission means that it needs its own cadre of cyber warriors. "So, we believe we have to have our own indigenous cyber experts; they initially will be focused almost exclusively on cyber defense."

The Space Force's new Spacepower Capstone Doctrine calls "Cyber Operations" one of the "spacepower disciplines" required for the new service to undertake is missions. The others are: "Orbital Warfare, Space Electromagnetic Warfare, Space Battle Management, Space Access and Sustainment, Military Intelligence, and Engineering/Acquisitions."

While Whiting didn't go there, the new doctrine also asserts that Space Force offensive operations could include attacks on adversary cyber networks. "Offensive operations seek to gain the initiative and may neutralize adversary space missions before they can be employed against friendly forces. Offensive operations are not limited to adversary counterspace systems and can also target the full spectrum of an adversary's ability to exploit the space domain, which includes targets in the terrestrial and cyber domains," the doctrine document states.

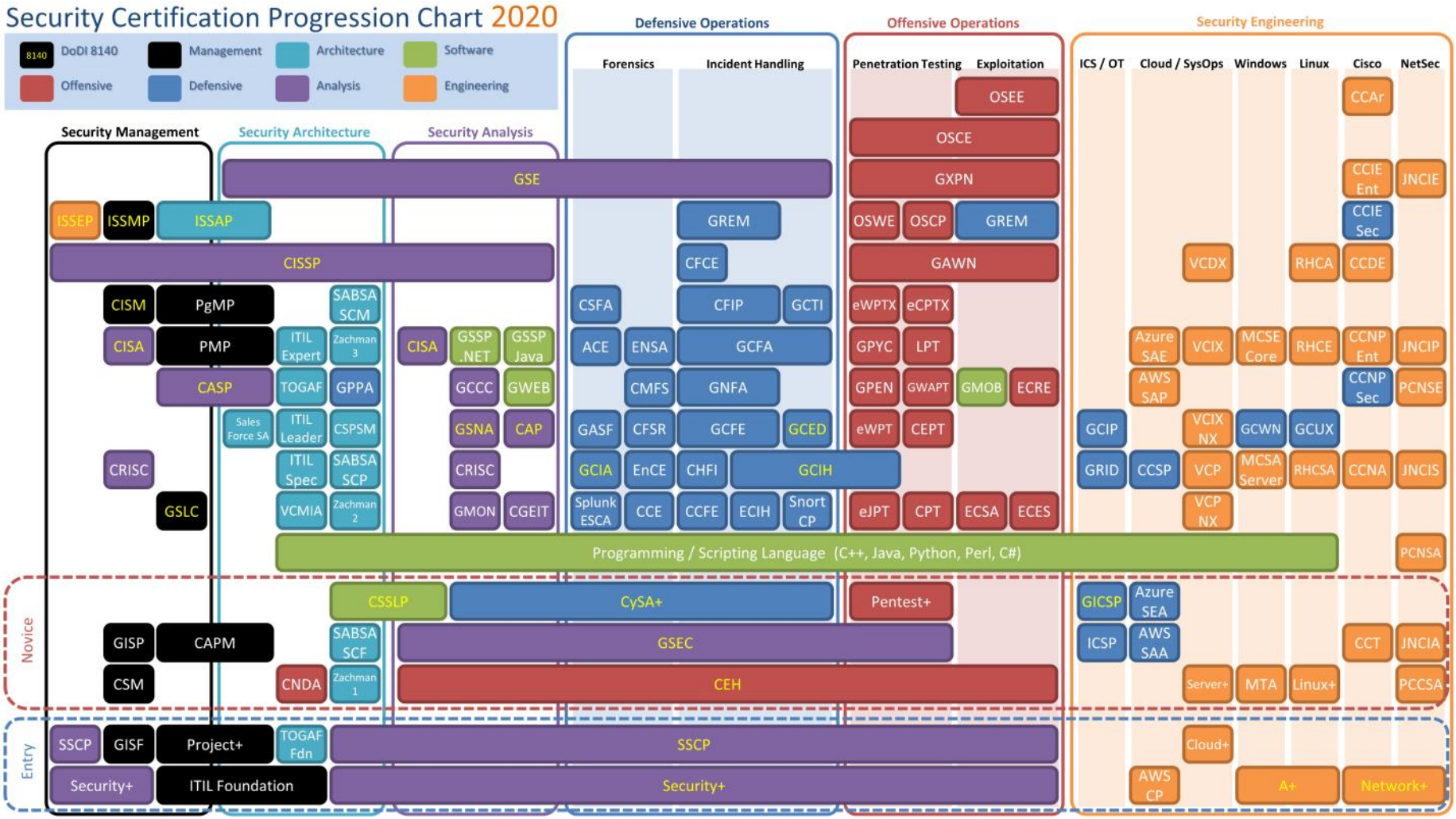
Read the rest here:

https://breakingdefense.com/2020/09/cyber-attack-most-likely-space-threat-maj-gen-whiting/

Provided by Kurt Danis, CISSP, ISSA-COS.

Comments by many IA practitioners may be read here:

https://www.reddit.com/r/cybersecurity/comments/e23ffz/security_certification_progression_chart_2020/



MENTORING PROGRAM

The ISSA-COS Mentoring Program provides a connection between individuals (mentees) seeking career guidance, industry information, or personal encouragement with individuals (mentors) who have an aptitude for sharing their career experiences, industry resources, and personal talents for the benefit of the mentee. Mentees derive from every conceivable background and exist at every stage of professional development. Mentoring sessions are designed to ensure the confidentiality, integrity, and availability of information shared between the participants.

To help facilitate the mentoring process, ISSA-COS has adopted the S.M.A.R.T. goal setting model to safeguard a consistent development process that is equally understood and honored by mentees and mentors alike. As such, the Mentoring Program supports the following objectives of ISSA-COS:

For more information about mentoring, email: *mentorship@issa-cos.org*

- Promote increased professional education opportunities for members
- Provide career guidance and professional development approaches
- Encourage balance between technical skillsets and soft skills such as time management, task management, workplace conduct, and business savvy
- Increase member knowledge of available resources designed to strengthen skillsets
- Encouraging an open exchange of Cybersecurity related techniques, approaches, and problem-solving skills
- Promote member education and awareness of Cybersecurity security issues and recommended strategies to combat the issues
- Providing opportunities for mentees and mentors to network with other professionals and share their lessons learned from their individual mentoring experiences.

Cyber Spotlight – PARTY!!

ISSA-COS is turning 30 in 2021!

Initiative to document ISSA-COS Chapter History

Interviews with past/current **Presidents**

Interviews with past/current **Board Members**

Interviews with past/current **General Members**

Interviews with **Community Partners**

DOD Cybersecurity Certification Body Moving Forward Despite Uncertain Funding

By Mariam,Baksh, NextGov, September 19, 2020

The first class of assessors being trained by a volunteer accreditation body established to implement the Defense Department's Cybersecurity Maturity Model Certification program should start receiving approval within the coming week, but may not have access to continuous monitoring to conduct initial audits, as the organization struggles to fund its operations.

"We don't have any external funds to pay for things that we needed, whether it was continuous monitoring, whether it was staff, whether it was insurance, all the normal business things we needed," said Chris Golden, a member of the board of directors for the accreditation body, or AB. "We've been struggling spending a significant amount of our time trying to figure those things out versus figuring out what the ecosystem is going to look like and training people and getting assessments going and those kinds of things."

Golden spoke along with Robert Metzger, an attorney who co-authored the MITRE report "Deliver Uncompromised" and has been a member of the Defense Science Board, during an event Friday hosted by the cybersecurity ratings company BitSight. BitSight has submitted a response to the accreditation body's request for proposal for a continuous monitoring solution, vice president of communications and government affairs Jake Olcott told *Nextgov.*

Deliver Uncompromised was among the first venues where the current method of approving defense contractors' security practices—taking the companies by their word—was deemed ineffective. In response, CMMC will require any defense contractor in possession of certain sensitive information to be audited by an independent third party.

Metzger has been a vocal critic of what he described as possible commercialization of the accreditation body but said expectations placed on the group by the Defense Department are unfeasible.

"We have to appreciate that the department of Defense has put the AB into a fairly difficult spot," he said. "This is a very difficult undertaking and they have given no money to the AB to do it. If there is a problem here, some of it may have been misjudgments that can be corrected by the AB, but some of it is because the funding model that the DOD has created strikes me as a lot more optimistic than realistic."

Read the rest here:

https://www.nextgov.com/cybersecurity/2020/09/dod-cybersecurity-certification-body-moving-forward-despite-uncertain-funding/168424/

Fewer than half of healthcare institutions met national cybersecurity standards last year

By Hailey Mensik, HealthcareDrive, September 17, 2020

The COVID-19 pandemic forced providers and patients to rapidly move care to virtual settings this year. Providers had just weeks to convert visits online and adopt the technology needed to do so, though temporarily loosened restrictions from CMS helped.

But the report shows even before the public health crisis, healthcare institutions' compliance with cybersecurity standards were sliding.

"In cybersecurity, if you are not improving, you are falling behind in managing your risks," the report's authors said. "The bad guys keep getting better, the technology more complex, and more of it is being deployed."

Among the healthcare organization clients CynergisTek analyzed, assisted living facilities had the highest NIST compliance at 96%, though it noted they don't typically have highly automated systems, frequently don't have EMRs, and only have minimal, "core systems."

Insurers and accountable care organizations had the next highest compliance, then business associates and hospitals and health systems. Physicians groups had the lowest compliance at 20%.

Looking at hospital type, academic medical centers had the highest compliance, followed by critical access hospitals, health systems and short-term acute care hospitals.

Read the rest here:

https://www.healthcaredive.com/news/CynergisTek-healthcare-cybersecurity-compliance-2019/585442/

DOD releases interim cybersecurity rule

By Lauren C. Williams, FCW, September 29, 2020

The Defense Department released an interim rule for its Cybersecurity Maturity Model Certification program that will require contractors to prove they are keeping up with key cybersecurity measures.

The rule, which goes into effect Nov. 30, was published in the Federal Register Sept. 29. Public comments will be collected until then and are expected to be considered when crafting the final rule.

Ellen Lord, DOD's top buyer, announced the rule's publication during a virtual keynote presentation at the Common Defense 2020 conference on defense industry base procurement.

"To ensure cybersecurity is also foundational for our partners in industry, the department created the Cybersecurity Maturity Model Certification or CMMC," Lord said. "Thereby requiring all DOD contracts by Oct. 21, 2025 -- five years from now -- to have some level of CMMC in each of those contracts."

The interim rule includes contracting language to amend the Defense Federal Acquisition Regulation Supplement that "requires contractors to apply the security requirements of NIST SP 800-171 to 'covered contractor information systems'...that are not part of an IT service or system operated on behalf of the government."

The interim rule effectively creates three levels for cybersecurity assessments -- basic, which is required to be eligible for award, medium and high, which can be conducted during the course of performance -- and two assessment tracks, one for NIST 800-171 that's effective now and one for CMMC, according to an analysis by the Wiley Rein law firm in Washington, D.C.

"Under this framework, contractors will be required to complete a self-assessment of their compliance with NIST SP 800-171 before they can receive DOD contracts," Wiley Rein wrote.

"For CMMC, the interim rule introduces the long-anticipated DFARS clause that sheds some light on how DOD contractors are expected to flow down the requirements to subcontractors. But the interim rule also highlights DOD's desire to continue developing the CMMC requirements outside the DFARS rulemaking process."

Read the rest here:

https://fcw.com/articles/2020/09/29/dod-interim-cyber-rule-released.aspx

Cybersecurity: Your supply chain is now your weakest link

By Danny Palmer, ZDNet, September 24, 2020

More than 80% of organisations have experienced a data breach as a result of security vulnerabilities in their supply chains, as cyber criminals take advantage of the poor security of smaller vendors as a means of gaining access to the networks of large organisations.

Research by cybersecurity company BlueVoyant found that organisations have an average of 1,013 vendors in their supplier ecosystem – and that 82% of organisations have suffered a data breach in the past 12 months due to cybersecurity weakness in the supply chain.

But, despite the risk posed by security vulnerabilities in the supply chain, a third of organisations have little to no indication if hackers had got into their supply chain, meaning that they may not find out that they've been the victim of an incident until it's too late.

Large companies are likely to be better protected than smaller companies, which means hackers are increasingly turning towards their suppliers as a means of infiltrating the network in a way that will often go unnoticed.

"Very often people think, well, what are our most critical suppliers and inevitably they end up with their top ten being some of the world's biggest names, like cloud providers. But that's not where the threat comes from," said Robert Hannigan, chairman of BlueVoyant International, told ZDNet.

"It's much more likely that the real threat is going to come from a much smaller company you've never heard of but which is connected to your network," said Hannigan, who was previously director of GCHQ.

Read the rest here:

https://www.zdnet.com/article/cybersecurity-your-supply-chain-is-now-your-weakest-link/

October is National Cybersecurity Awareness Month

By Staff, CISA, October 1, 2020

October is National Cybersecurity Awareness Month (NCSAM), which is a collaborative effort between the Cybersecurity and Infrastructure Security Agency (CISA) and its public and private partners—including the National Cyber Security Alliance—to ensure every American has the resources they need to stay safe and secure online. This year's theme, "Do your Part. #BeCyberSmart.," encourages individuals and organizations to take proactive steps to enhance cybersecurity and protect their part of cyberspace.

CISA encourages individuals and organizations to review the NCSAM 2020 page for ways to participate in and promote NCSAM.

NIST guide to help orgs recover from ransomware, other data integrity attacks

By Zeljka Zorz, HelpNetSecurity, September 24, 2020

The National Institute of Standards and Technology has published a cybersecurity practice guide enterprises can use to recover from data integrity attacks, i.e., destructive malware and ransomware attacks, malicious insider activity or simply mistakes by employees that have resulted in the modification or destruction of company data (emails, employee records, financial records, and customer data).

Ransomware is currently one of the most disruptive scourges affecting enterprises. While it would be ideal to detect the early warning signs of a ransomware attack to minimize its effects or prevent it altogether, there are still too many successful incursions that organizations must recover from.

Special Publication (SP) 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events can help organizations to develop a strategy for recovering from an attack affecting data integrity (and to be able to trust that any recovered data is accurate, complete, and free of malware), recover from such an event while maintaining operations, and manage enterprise risk.

The goal is to monitor and detect data corruption in widely used as well as custom applications, and to identify what data way altered/corrupted, when, by whom, the impact of the action, whether other events happened at the same time. Finally, organizations are advised on how to restore data to its last known good configuration and to identify the correct backup version.

Read the rest here:

https://www.helpnetsecurity.com/2020/09/24/nist-guide-recover-ransomware/?web_view=true

Update Your Profile!

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

CISA Releases Telework Essentials Toolkit

By Staff, CISA, September 30, 2020

The Cybersecurity and Infrastructure Security Agency (CISA) has released the Telework Essentials Toolkit, a comprehensive resource of telework best practices. The Toolkit provides three personalized modules for executive leaders, IT professionals, and teleworkers. Each module outlines distinctive security considerations appropriate for their role:

- Actions for executive leaders that drive cybersecurity strategy, investment and culture
- Actions for IT professionals that develop security awareness and vigilance
- Actions for teleworkers to develop their home network security awareness and vigilance

CISA encourages users and administrators to review the Telework Essentials Toolkit and the CISA Telework page for more information.

CISA Data Shows Federal Civilian Agencies Faster Than Industry at Patching

By Mariam,Baksh, NextGov, September 17, 2020

An analysis of data collected by the Cybersecurity and Infrastructure Security Agency shows civilian government agencies are doing better than private sector owners and operators of critical infrastructure when it comes to a major indicator of adherence to basic cybersecurity practices.

"For the federal civilian executive branch, we've seen patching timeframes consistently hold at 15 days for critical vulnerabilities and 30 days for high," said Boyden Rohner, associate director of vulnerability management at CISA. "However, outside of the federal civilian executive branch, in other critical infrastructures, the timeframes to patch have been largely longer."

Rohner used data gathered from entities subscribing to CISA services such as incident response and vulnerability assessment to share insights and predictions for 2020 on Wednesday as part of CISA's third annual cybersecurity summit.

CISA and the Office of Management and Budget recently finalized instructions for federal agencies to lay out the welcome mat for security researchers who can identify vulnerabilities in their systems. And the agency is establishing a platform it can use to hold agencies accountable to expected patching times for vulnerabilities brought to their attention. But the majority of the nation's critical infrastructure—about 85% according to the Government Accountability Office— is privately controlled.

Rohner encouraged organizations to continue targeting the low-hanging fruit of known vulnerabilities in their management of risk.

The bad news, she said, is that "33 % of critical infrastructure operates a potentially risky service exposed to the internet and 52% of critical infrastructure has a vulnerability that has a known exploit available." But there is also good news. "We're seeing a reduction of actionable, exploitable vulnerabilities," Rohner said. "This means entities are prioritizing their vulnerability management activities effectively."

Following an announcement Wednesday, CISA will now play a greater role in determining what even counts as a vulnerability within some areas of the private sector. The agency has been approved by the Common Vulnerabilities and Exposures program maintained by the MITRE corporation to act as a supervisory, or "top-level," CVE numbering authority for industrial control systems and medical devices.

"This designation as a Top-Level Root enables the rapid identification and resolution of issues specific to those environments," said Chris Levendis, CVE Program Board Member and a principal systems engineer at MITRE. "This is consistent with the CVE Program's federated growth strategy to scale the CVE Program in a sustainable, stakeholder driven way."

CISA will initially contribute to and oversee the vulnerability identification activities of seven entities, including Siemens and Johnson Controls.

Read the rest here:

https://www.nextgov.com/cybersecurity/2020/09/cisa-data-shows-federal-civilian-agencies-faster-industry-patching/168585/

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: Steven Mulig
- Deputy: **Vacant**

Vice President of Training: Mark Heinrich
- Deputy: Phebe Swope

Member at Large: Art Cooper
Member at Large: Jim Blake
Member at Large: James Asimah
Member at Large: Dennis Kater

Committee Chairs:

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

**** 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

This Hacked Coffee Maker Demands Ransom and Demonstrates a Terrifying Implication About the IoT

By Alyse Stanley, Gizmodo, September 26, 2020

It's no secret that the Internet of Things is full of insecure gadgets. All you need is one high profile incident to be flooded with terrifying headlines about how everything from robotic vacuum cleaners to smart sex toys can be hacked to spy on you. However, apparently some devices like Smarter's IoT coffee machine can also be reprogrammed to go haywire and demand ransom from unsuspecting users.

This week, Martin Hron, a researcher with the security firm Avast, reverse engineered a $250 Smarter coffee maker as part of a thought experiment to potentially uncover an important flaw in the infrastructure of smart devices.

Read the rest here:

https://gizmodo.com/this-hacked-coffee-maker-demands-ransom-and-demonstrate-1845191662

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