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

ISSA-COS NEWSLETTER
VOLUME 10 NUMBER 2
FEBRUARY 2021

Colorado Springs, Colorado

FBI issues alert amid Florida Oldsmar water-treatment hacking investigation

By Michael Ruiz, Stephanie Pagones, Fox News, February 9, 2021

"The FBI has observed corrupt insiders and external cyber actors using desktop sharing software to victimize targets in a range of organizations, including those in the critical infrastructure sectors," the FBI said in a threat overview alert Tuesday evening.

The overview warned that TeamViewer software, which has legitimate uses as a desktop sharing and remote access platform, was being exploited by hackers to "exercise remote control over computer systems" in a way that made it "functionally similar" to Trojan-horse style viruses that infect a computer from within and grant remote entry to hackers.

Because TeamViewer does have legitimate uses and is not a virus, the FBI warned that its abuse can appear less suspicious to system administrators.

Additionally, the bureau warned that dated systems like Microsoft's Windows 7 operating system, nearing their end of their useful lives, are at risk of becoming even more vulnerable once the manufacturer ceases product support.

Authorities are recommending using multi-factor authentication, strong passwords, up-to-date software and other security measures.

Additionally, the FBI is recommending workers be trained in how to attempt social engineering attempts -- in which malicious actors use false identities to coax victims into leaking information or passwords or compromising their own systems from within.

One example would be a hacker posing as a member of a company's IT department and instructing a worker to give TeamViewer access so they could infiltrate the system.

In the Oldsmar case, hackers allegedly obtained access to the facility's supervisory control and data acquisition system -- software that has near-complete control over the plant.

Oldsmar is approximately 15 miles from Tampa and is home to just under 15,000 people.

"Right now, we do not have a suspect identified but we do have leads that we're following," Gualtieri said Monday. "We don't know right now whether the breach originated from within the United States or outside the country. We also do not know why the Oldsmar system was targeted and we have no knowledge of any other systems being unlawfully accessed."

The hacker first breached the system at approximately 8 a.m. Friday but only did so momentarily before logging off. A plant operator on duty noticed the "brief" remote access, but wasn't particularly concerned because supervisors "regularly" access the computers remotely to monitor the system, officials said.

Read the rest here:

https://www.foxnews.com/us/fbi-florida-authorities-tips-water-treatment-hacking

The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our members, and do not constitute or imply endorsement by ISSA or the Colorado Springs Chapter of ISSA of any entity, event, product, service, or enterprise.

Who's Making All Those Scam Calls?

By Yudhijit Bhattacharjee, New York Times, January 27, 2021

One afternoon in December 2019, Kathleen Langer, an elderly grandmother who lives by herself in Crossville, Tenn., got a phone call from a person who said he worked in the refund department of her computer manufacturer. The reason for the call, he explained, was to process a refund the company owed Langer for antivirus and anti-hacking protection that had been sold to her and was now being discontinued. Langer, who has a warm and kind voice, couldn't remember purchasing the plan in question, but at her age, she didn't quite trust her memory. She had no reason to doubt the caller, who spoke with an Indian accent and said his name was Roger.

He asked her to turn on her computer and led her through a series of steps so that he could access it remotely. When Langer asked why this was necessary, he said he needed to remove his company's software from her machine. Because the protection was being terminated, he told her, leaving the software on the computer would cause it to crash.

After he gained access to her desktop, using the program TeamViewer, the caller asked Langer to log into her bank to accept the refund, $399, which he was going to transfer into her account. "Because of a technical issue with our system, we won't be able to refund your money on your credit card or mail you a check," he said. Langer made a couple of unsuccessful attempts to log in. She didn't do online banking too often and couldn't remember her user name.

"I'm going to give you the password to unlock your PC because they use the same password every time," he said. "If you type 4-5-2-1, you'll unlock it."

Frustrated, the caller opened her bank's internet banking registration form on her computer screen, created a new user name and password for her and asked her to fill out the required details — including her address, Social Security number and birth date. When she typed this last part in, the caller noticed she had turned 80 just weeks earlier and wished her a belated happy birthday. "Thank you!" she replied.

After submitting the form, he tried to log into Langer's account but failed, because Langer's bank — like most banks — activates a newly created user ID only after verifying it by speaking to the customer who has requested it. The caller asked Langer if she could go to her bank to resolve the issue. "How far is the bank from your house?" he asked.

A few blocks away, Langer answered. Because it was late afternoon, however, she wasn't sure if it would be open when she got there. The caller noted that the bank didn't close until 4:30, which meant she still had 45 minutes. "He was very insistent," Langer told me recently. On her computer screen, the caller typed out what he wanted her to say at the bank. "Don't tell them anything about the refund," he said. She was to say that she needed to log in to check her statements and pay bills.

Langer couldn't recall, when we spoke, if she drove to the bank or not. But later that afternoon, she rang the number the caller had given her and told him she had been unable to get to the bank in time. He advised her to go back the next morning. By now, Langer was beginning to have doubts about the caller. She told him she wouldn't answer the phone if he contacted her again.

"Do you care about your computer?" he asked. He then uploaded a program onto her computer called Lock My PC and locked its screen with a password she couldn't see. When she complained, he got belligerent. "You can call the police, the F.B.I., the C.I.A.," he told her. "If you want to use your computer as you were doing, you need to go ahead as I was telling you or else you will lose your computer and your money." When he finally hung up, after reiterating that he would call the following day, Langer felt shaken.

Minutes later, her phone rang again. This caller introduced himself as Jim Browning. "The guy who is trying to convince you to sign into your online banking is after one thing alone, and that is he wants to steal your money," he said.

Read the rest here:

https://www.nytimes.com/2021/01/27/magazine/scam-call-centers.html?searchResultPosition=1

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

Our membership is hanging in at ~334 members as of the end of January 2021. 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—January	
Patrick Pendergest	Sothorn Meng Khaul
Dr. Gurvirender Tejay	Jonathon Edward McNulty
Bret Friedrich	

Thanks,

Steven Mulig

VP-Membership
membership@issa-cos.org

Update Your Profile!

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

The Weak Point in the CIA Triad – “Integrity”

By Mike Crandall, Vice-President, ISSA-COS, January 25, 2021

Cybersecurity often described using the CIA Triad. The CIA stands for Confidentiality, Integrity, and Availability and these are the three elements of data that information security tries to protect. If we look at the CIA triad from the attacker’s viewpoint, they will seek to compromise confidentiality by stealing data, integrity by manipulating data and availability by deleting data or taking down the systems that host the data.

By and far, most attacks have been focused on disrupting confidentiality or availability, so defense mechanisms and training has also been focused there. The number of data breaches has skyrocketed and there is a flourishing market for stolen data including personal health information, credit card numbers, social security numbers, advertising lists, and proprietary technology. We also see many attacks on availability through Denial of Service and the surge of Ransomware attacks.

Integrity attacks are when data is manipulated, changed, or deleted and to mitigate this risk encryption is often used. In fact, most equate Integrity with encryption but what about those other attacks where log files are deleted or altered to hide the tracks of those penetrating a system. In fact, many rootkits are specifically designed to alter logs to remove any evidence of the rootkits’ installation or execution. NIST SP 800-92 “Guide to Computer Security Log Management” specifically calls for the Integrity protection of log data at rest and in transit. The publication does not, however, provide any specific techniques to accomplish this task.

Integrity is a cornerstone of business, governance, and law enforcement, as well as a dedicated principle of their underlying computing systems. Those systems initially evolved from the days of host-based mainframes to Client/Server computing. Transaction Processing, associated reports and Static Files were the dominant systems and data types of both eras. Malicious hacking in support of academic security research and digital fraud followed soon after, ushered into the mainstream by the Morris Worm virus of 1988. Four years later, innovative research from undergrad Gene Kim at Purdue University released the popular tripwire tool and pioneered the category of File Integrity Monitoring (FIM). It became an early foundation for computer security (intrusion detection), audits, forensics, and mainstream regulatory compliance requirements such as SOX-404 and PCI-DSS, to name a few. FIM is focused on static files and since log files are ever changing, they are more difficult to provide Integrity for.

By 2007, Client/Server computing had reached its zenith and the disruptive iPhone release catalyzed existing Web Computing demand for a wider **Variety**, greater **Volume** and **Velocity** (3 Vs) of data types, with associated new databases and processing systems. The terms Big Data and NoSQL were coined to cover the cambrian explosion of new software for this demand, and the introduction of Cloud computing proved to be the dominant operational model to deliver solutions satisfying this demand. But one critical ‘V’ was left behind in this revolution - **Veracity**.

Agile data is active, constantly capturing, transforming, and moving information. Static file integrity monitoring (FIM) was never designed to represent the proper state of dynamic data flowing through an agile big data system in the cloud, or at the edge. Yet regulatory requirements in the Public Sector, Financial Services, Healthcare, Retail, Communications, Transportation, and other industry verticals have only grown since the invention of FIM, almost 30 years ago. We need a new Integrity Monitoring Architecture which works across old and new data types and systems.

The future of Integrity monitoring is eXtended Integrity Monitoring (XIM) which is a 21st century design for integrity monitoring, built upon the original 20th century FIM requirements, updated for modern social, business, security and regulatory needs. Security event logs are the lifeblood of cyber security, Digital Forensics and Incident Response (DFIR) and compliance in a 21st century organization. Security Incident and Event Management (SIEM) solutions are popular with Enterprises and Managed Security Service Providers (MSSPs) which operate Security Operations Centers (SOCs). However, log tampering jeopardizes value of the entire SIEM solution, reducing SOC efficiency and productivity, exposing related organizations to increased cyber risk.

XIM creates a chain of custody by registering a data source such as in-memory data, databases, files, objects & logs from IAM, PAM, EDR, XDR & SIEM to a RESTful API. In the registration process, the hash of the data source is anchored to a Distributed Ledger Technology (DLT) hosted on AWS, locally, or a public ledger. Once a hash is registered on the DLT, it can be used as a decentralized verification of current hashes for any item within your network. The simple Boolean response from the RESTful Verify() API will provide a response of true if the registered and current hashes match, or false if they don’t. Never an intermediary state, always deterministic.

The performance, granularity, domain separation, efficiency, robustness, and architecture of XIM solutions enable complete agile integrity monitoring (veracity) of data pipelines like these, regardless of volume, variety or velocity. It is time focus on all THREE pillars of the CIA Triad with XIM methodology and emerging technology can make that possible.

Keeping Up

By Pat Sheehan, IT Chairman, ISSA-COS, Janyary 26, 2021

As cybersecurity professionals, we're all busy. At our jobs we're expected to know some system admin, some helpdesk, some network engineering, and something about ANYTHING that has "cyber", "breach", "dark web", or "RMF" in its title or description. Then if you're like me, you're also the level one- and two- computer technician for all your family and friends. They also have some expectation that you'll know about anything that is sort of "techie". "Techie" can include everything from drones, to ring doorbells, to self-driving cars. With all these job and personal demands for my time I feel like I'm missing some cybersecurity news and if I feel this way, maybe some of you feel this way as well.

I've decided that I need to increase my efforts to be more cybersecurity news aware and tech informed, with the emphasis on cybersecurity. But where to start? I'm taking the approach of a professional self-improvement effort; much like getting a new certification or learning a new skill. Like many self-improvement efforts, the key (in my humble opinion) to lasting change is incremental, sustainable changes to your everyday behaviors.

I have set aside (and what I want you to also) a small amount of time every day to read cybersecurity news. Now most of us read news on our phone, on a website, watch it on the television, but usually that's a "news of the world" kind of thing. Keep doing that. However in addition, I want you to actually schedule time in your calendar to read the cybersecurity news of the day. Schedule fifteen to thirty minutes every day catching up on our profession; that's the goal.

To help you and me in this endeavor, here is a list of good cybersecurity news resources. This list of sites came from an FBI newsletter I used to get, but they aren't producing it at this time. I went through several back issues and extracted the most prevalent sources used in those newsletters and listed them below, in no particular order. As you read through the cybersecurity news of the day, you'll see the big stories that span across multiple websites (e.g. SolarWinds hack). But hopefully, you'll also find some things that are really interesting but not in the mainstream. Enjoy!

https://www.hackread.com/

https://www.techrepublic.com/

https://www.securityweek.com/

https://arstechnica.com/

https://www.infosecurity-magazine.com/

https://www.bleepingcomputer.com/

https://blog.malwarebytes.com/category/malwarebytes-news/

https://threatpost.com/

https://cyware.com/cyber-security-news-articles

https://techcrunch.com/

https://www.zdnet.com/

https://securityboulevard.com/

https://thehackernews.com/

https://www.theregister.com/security/

https://www.cyberscoop.com/

Finishing Up My Tour at the ISSA-COS Speakers Bureau

By Jay Carson, (Formerly) ISSA-COS Speakers Bureau Committee Chairperson

I had a great time for 2+ years serving as your Speakers Bureau committee chairperson, but I am now on the ISSA-COS Board as a Member-at-Large. I leave the Speakers Bureau team in outstanding hands!

The purpose of this article is to summarize the presentations October 2020 - January 2021, with each synopsis provided by the presenters and/or ISSA-COS leadership. If you wish to contact the presenters and have any challenges, I may be able to assist at member-at-large4@issa-cos.org. From the April 2nd through the January 19th offerings (now back to being called chapter meetings!), the ISSA-COS Board and Key Personnel team have been able to conduct 24 sessions, offering members up to 36 hours of potential continuing education credits. COVID did not stop ISSA-COS from providing service!

The April-September programs were detailed in previous newsletters.

October

1. Date: 8 October 2020. **Speaker**: Rear Admiral (ret.) Hank Bond, Chief Executive Officer and Co-Founder, ForceNow, LLC. Topic: Missing in Action: Critical Thinking in the Cyber Security Solution Space. Synopsis: How using two physical-domain analogues of warfighting concept development may stimulate critical thinking about the cybersecurity solution space at a metalevel.

2. Date: 22 October 2020. **Speakers**: Moderator: Ms. Vanessa Johnson, President, AFCEA-RMC. Panel Members: Mr. Thomas Russell, Director of Education, NCC. Ms. Jennifer Kurtz, Director, Manufactures Edge. Mr. James Lacey, Director, JMark Services. Topic: National Cybersecurity Awareness Month. Synopsis: Panel Discussion: Adjusting to a Virtual Lifestyle: Impacts and Predictions on Work, Commerce, and Education.

November

3. Date: 5 November 2020. **Speaker**: Mr. Michael Wylie, MBA, CISSP

Director of Cybersecurity Services, Richey May Technology Solutions. Topic: Intro to Malware Analysis & Response (MA&R) Part 2. Synopsis: Back by popular demand, Mike briefly reviewed his 6 August presentation and took us further into Basic Dynamic Analysis, Memory Analysis, and Reverse Engineering / Manual Code Review. IT and Cybersecurity professionals learned the basic workflow and techniques to safely analyze the characteristics and behaviors of malware. Attendees walked away with practical techniques and methodologies that can be immediately applied to statically and dynamically analyzing software with an emphasis on malicious software.

December

4. Date: 3 December 2020. **Speakers**: William J. (Jay) Carson, Security+, CIPP/E, ISSA-COS, IAPP Member, Privacy Consultant to Semper Sec LLC. Mark L. Spencer, CISSP, ISSA Distinguished Fellow, ISSA Honor Roll, President Emeritus ISSA-COS. Colleen Murphy, CISSP, C|CISO, ISSA Fellow, Past President ISSA-COS. Justin Whitehead, Founder at Digital Silence (SDVOSB). Erin Beffa, OSINT Practice Lead for Digital Silence. Rob Carson, CISSP, CISA, Founder, Semper Sec LLC. Topic: Cyber Bubble Wrap: How to apply cybersecurity to defend senior citizens. Synopsis: Many cybersecurity professionals have senior citizens among family/friends. Do we engage our cybersecurity skills to keep 'Mom' safe? By being active online, especially with COVID isolation, homebound seniors can stay mentally active and engaged. However, as a group, seniors often have financial/property resources, are more trusting, and are more easily deceived by cyber predators.

5. Date: 17 December 2020. **Speaker**: Ms. Erin Miller, Vice President of Operations, Space ISAC, NCC. Topic: Space ISAC – An Overview of 2020 and a Preview of 2021. Synopsis: The Space ISAC serves to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information. Ms. Miller provided ISSA-COS with an update of recent and future events associated with the Space ISAC.

January

6. Date: 19 January 2021. **Speaker**: Jeremy Druin, OSCP, GXPN-GOLD, GPEN-GOLD, GMOB, GWAPT-GOLD, GCIH-GOLD, GSEC, GSIF, Sec+. Principal Cybersecurity Architect at UPS. Owner, Ellipsis Information Security, LLC. Education Director for the Louisville ISSA chapter. Topic: The Best Passwords are not Passwords: Modern Password Policies. Synopsis: Organizations get comfy with password policies but may not stop to consider whether the policy is actually effective. Which characteristics make passwords "secure"? How do we know if our policy is broken? We looked at what password policies are effective, which are not as important as everyone seems to think, and which might be harmful. Mr. Druin can be reached at jeremy@ellipsisinfosec.com.

The 2021 Fellows Cycle is now OPEN!

The suspense to apply is 30 April 2021

Submit your application for the ISSA Fellows Program *ASAP*

Senior Member

Any member can achieve Senior Member status, the first step in the Fellow Program. The Colorado Springs Chapter has over 50 members who have attained Senior Member status! Are you ready to join them? Requirements are as follows:

- 5 years ISSA membership (NOTE: membership does not have to be contiguous or in the same chapter. A break in your membership is ok, you just need a total of 5 years)
- 8 years relevant professional experience

Your application must be endorsed by a Chapter Board member. If you have any questions about **Senior Member** applications, please contact any Member-at-Large:

- Art Cooper: member-at-large1@issa-cos.org
- Jim Blake: member-at-large2@issa-cos.org
- James Asimah: member-at-large3@issa-cos.org
- Jay Carson: member-at-large4@issa-cos.org

Fellow

Members need to meet additional criteria before they may be considered for Fellow status. The Colorado Springs Chapter has 12 members who have attained Fellow status! Are you ready to join them? Requirements for Fellow recognition are as follows:

- 8 years ISSA membership (***NOTE:*** membership does not have to be contiguous or in the same chapter. A break in your membership is ok, you just need a total of 8 years)
- 12 years relevant professional experience
- 3 years volunteer leadership in ISSA
- 5 years significant performance in the profession

You must be nominated by a current Fellow or Distinguished Fellow

Distinguished Fellow

Members need to meet additional criteria before they may be considered for Distinguished Fellow status. The Colorado Springs Chapter has 6 members who have attained Distinguished Fellow status! Are you ready to join them? Requirements for Fellow recognition are as follows:

- 12 years ISSA membership (***NOTE:*** membership does not have to be contiguous or in the same chapter. A break in your membership is ok, you just need a total of 12 years)
- 16 years relevant professional experience
- 5 years sustained volunteer leadership in ISSA
- 10 years documented exceptional service to the security community

You must be nominated by a current Distinguished Fellow

If you have any questions about **Fellow** or **Distinguished Fellow** applications, please contact the Past Presidents at: Past-President@ISSA-COS.org

ISSA-COS
2021 Schedule of Events

Monthly Events

Chapter Meetings (6:00 – 7:30 PM) [1]

Tuesday, February 16, 2021 [2]
March – Quarterly/Annual Events
Tuesday, April 20, 2021 [3]
Tuesday, May 18, 2021 [3]
June – Quarterly/Annual Events
Tuesday, July 20, 2021 [3]
Tuesday, August 17, 2021 [3]
September – Quarterly/Annual Events
Tuesday, October 19, 2021 [3]
Tuesday, November 16, 2021 [3]
December – Quarterly/Annual Events

[1] Light Dinner Provided @ 5:30 PM
[2] Virtual Meeting; Recorded Playback Available
[3] In-person Meeting; Recorded Playback Available

Mini – Seminars (9:00 – 12:00 PM) [1]

Saturday, January 23, 2021 [2]
Saturday, February 20, 2021 [2]
March – Quarterly/Annual Events
Saturday, April 24, 2021 [3]
Saturday, May 22, 2021 [3]
June – Quarterly/Annual Events
Saturday, July 24, 2021 [3]
Saturday, August 21, 2021 [3]
September – Quarterly/Annual Events
Saturday, October 23, 2021 [3]
Saturday, November 13, 2021 [3]
December – Quarterly/Annual Events

[1] Continental Breakfast Provided @ 8:30 AM
[2] Virtual Meeting; Recorded Playback Available
[3] In-person Meeting; Recorded Playback Available

Quarterly Events

Virtual Security + CE Reviews

Saturday, March 6, 2021
Saturday, March 13, 2021
Saturday, March 20, 2021

Saturday, September 11, 2021
Saturday, September 18, 2021
Saturday, September 25, 2021

Cyber Focus Symposium (CFS)

April 2021
CFS Girl Scout Cyber Camp

April 20-22, 2021
CFS Job Fair
CFS Capture-the-Flag Challenge
CFS Conference

Virtual CISSP Review

Saturday, June 5, 2021
Friday, June 11, 2021
Saturday, June 12, 2021

Saturday, June 19, 2021
Friday, June 25, 2021
Saturday, June 26, 2021

Peak Cyber Symposium (PCS)

September 2021
PCS Girl Scout Cyber Camp

September 14 – 16, 2021
PCS Job Fair
PCS Capture-the-Flag Challenge
PCS Conference

(Continued on page 9)

Annual Events

[3] Annual Cyber SIG Summit	>>	Friday, June 18, 2021 (1:00 – 5:00 PM)
[4] Annual Cyber Social	>>	Friday, June 18, 2021 (5:00 – 9:00 PM)
Annual Chapter Elections	>>	Oct – Nov 2021 (Details TBA)
[4] Annual STAR Awards	>>	Friday, December 3, 2021 (5:00 – 9:00 PM)

[2] Virtual Meeting; Recorded Playback Available | [3] In-person Meeting; Recorded Playback Available | [4] In-person Meeting Only

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

Huawei's HarmonyOS: "Fake it till you make it" meets OS development

By Ron Amadeo, ArsTechnica, February 2, 2021

Huawei is China's—and formerly the world's—largest smartphone vendor, and over the past 18 months, it learned an important lesson: the company can't rely on the US supply chain. In 2019, the US government banned US exports to Huawei, which cut the company off from access to most chip and software suppliers. Building a phone is hard without access to key parts and apps. Huawei's latest Q4 2020 numbers show its phone sales in free fall, dropping 42 percent year-over-year.

Because of this, Huawei wants independence from the worldwide smartphone supply chain. While hardware independence is something the company needs to work on, Huawei also needs to get free of Google's software. So, as many companies have tried to do before it, Huawei hopes to make an Android killer.

The company's attempt at an in-house OS is called "HarmonyOS" (also known as "HongmengOS" in China). "Version 2" was released in December, bringing "beta" smartphone support to the operating system for the first time. Can Huawei succeed where Windows Phone, Blackberry 10, Sailfish OS, Ubuntu Touch, Firefox OS, Symbian, MeeGo, WebOS, and Samsung's Tizen have all tried and failed?

To hear Huawei tell the story, HarmonyOS is an original in-house creation—a defiant act that will let the company break free of American software influence. Huawei's OS announcement in 2019 got big, splashy articles in the national media. CNN called HarmonyOS "a rival to Android," and Richard Yu, the CEO of Huawei's consumer business group, told the outlet that HarmonyOS "is completely different from Android and iOS." Huawei President of Consumer Software Wang Chenglu repeated these claims just last month, saying (through translation), "HarmonyOS is not a copy of Android, nor is it a copy of iOS."

That makes HarmonyOS sound super interesting. Naturally, we had to take a deep dive.

After getting access to HarmonyOS through a grossly invasive sign-up process, firing up the SDK and emulator, and poring over the developer documents, I can't come to any other conclusion: HarmonyOS is essentially an Android fork. The way that Huawei describes the OS to the press and in developer documents doesn't seem to have much to do with what the company is actually shipping. The developer documents appear almost purposefully written to confuse the reader; any bit of actual shipping code to which you hold up a magnifying glass looks like Android with no major changes.

The phrase "fake it till you make it" is often given as motivational advice, but I've never seen it applied to OS development before. If you've ever seen a modern Huawei Android phone, HarmonyOS is largely the same thing... with a few strings changed. So while there's not much new to see, we can at least dissect HarmonyOS and debunk some of Huawei's claims about its "brand-new" operating system.

Read the rest here:

https://arstechnica.com/gadgets/2021/02/harmonyos-hands-on-huaweis-android-killer-is-just-android/

2020 Operations

ANNUAL AUDIT COMMITTEE

Committee Chair	Chris Edmondson

IT COMMITTEE

Committee Chair	Pat Sheehan
Committee Member	April Frost
Committee Member	Wayne Lo

SPEAKERS BUREAU COMMITTEE

Committee Chair	Jay Carson
Committee Member	Marcelle Licciardi

MENTORING COMMITTEE

Committee Chair	Carissa Nichols

TRAINING COMMITTEE

Committee Chair	Mark Heinrich
Committee Member – Instructors	Multiple
Committee Member – Facilitators	Multiple
Committee Member – Curriculum Authors	Multiple

MEDIA/NEWSLETTER COMMITTEE

Newsletter Committee Chair	Don Creamer
Photographer	Warren Pierce
Graphic Artist	Aaron Johnson

Girl Scouts Cyber Badge Camp

Girl Scouts Program Coordinator	Anna Parrish
PPCC Intern – Curriculum Author	Zavier Morales
PPCC Intern – Curriculum Author	Paul Baumgarten
PPCC Intern – Curriculum Author	Matt Huyge

ANNUAL ELECTION COMMITTEE

Committee Chair	Colleen Murphy
Committee Member	Frank Gearhart
Committee Member	Mark Spencer
Committee Member	Pat Laverty

MURRAY SECURITY SERVICES
NCC NATIONAL CYBERSECURITY CENTER
Colorado SBDC TECHSOURCE
COLORADO SPRINGS OLYMPIC CITY USA
women in cybersecurity WiCyS
Colorado Springs CHAMBER & EDC
PIKES PEAK COMMUNITY COLLEGE
Colorado Technical University
BLOCKFRAME
COLORADO PTAC
HANDSHAKE LEADERSHIP
ISSA Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org
Discover Goodwill
FIRMA
ManufacturersEDGE
Pikes Peak BUSINESS & EDUCATION ALLIANCE
PIKES PEAK WORKFORCE CENTER
UCCS
INFO~TECH RESEARCH GROUP
U.S. AIR FORCE ACADEMY
(ISC)² OFFICIAL CHAPTER
AFCEA Rocky Mountain Chapter
CSBJ
COLORADO SPRINGS WORLD AFFAIRS COUNCIL

ISSA-COS SALUTES ALL OUR CURRENT **COMMUNITY PARTNERS!**

THANK YOU FOR ALL YOU DO TO SUPPORT OUR CHAPTER AND OUR COMMUNITY!

TOGETHER WE ARE STRONGER

WWW.ISSA-COS.ORG

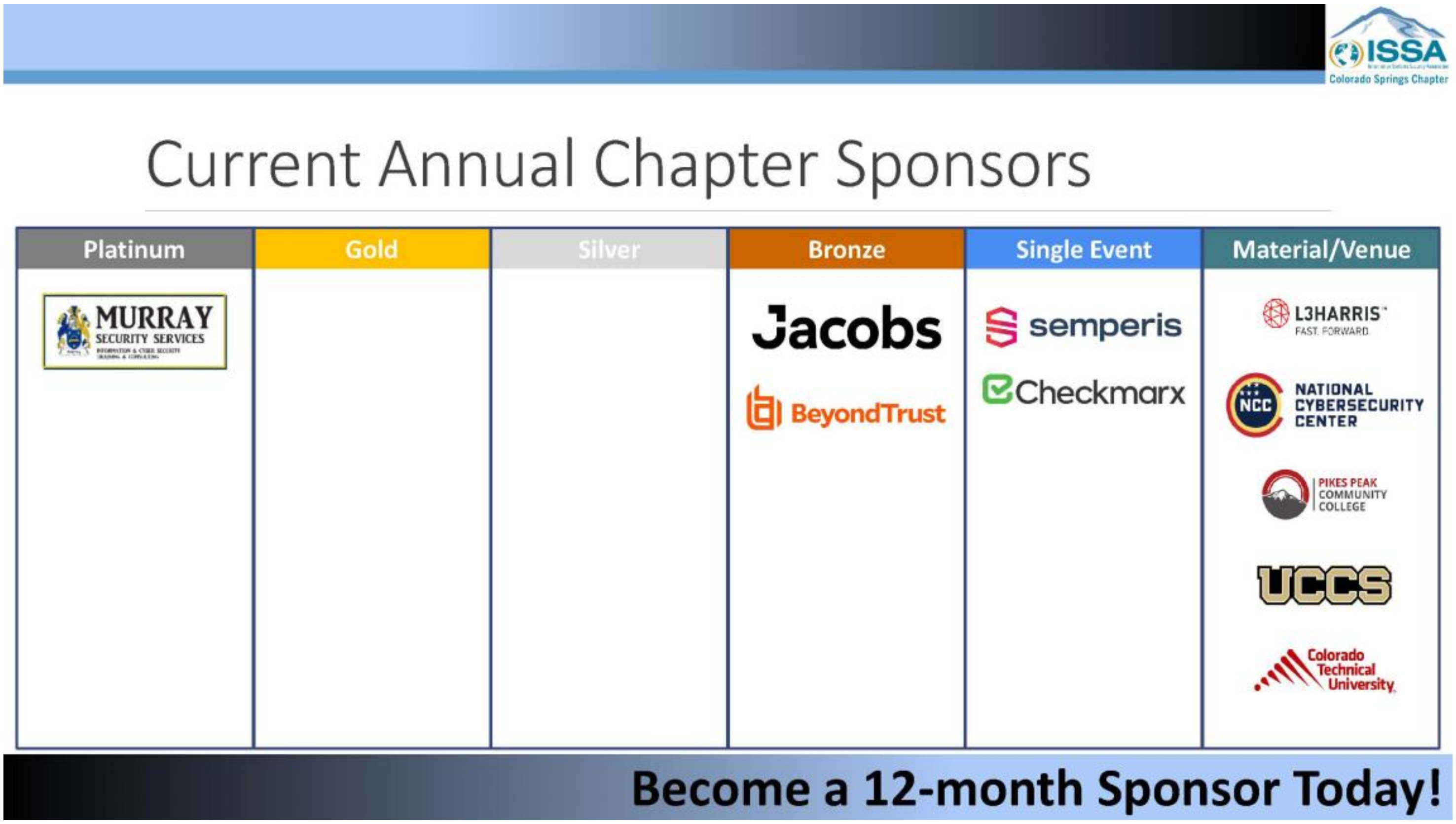
Strategic Partners

National Cyber Exchange

iapp

Discover Goodwill Southern & Western Colorado

Info~Tech Research Group



Current Annual Chapter Sponsors

Platinum	Gold	Silver	Bronze	Single Event	Material/Venue
Murray Security Services			Jacobs BeyondTrust	semperis Checkmarx	L3Harris Fast. Forward National Cybersecurity Center Pikes Peak Community College UCCS Colorado Technical University

Become a 12-month Sponsor Today!

NSA Cybersecurity Directorate Releases 2020 Year in Review

By CISA, Original release date: January 12, 2021

The National Security Agency (NSA) Cybersecurity Directorate has released its 2020 Year in Review, outlining key milestones and mission outcomes achieved during NSA Cybersecurity's first full year of existence. Highlights include NSA Cybersecurity's contributions to the 2020 elections, Operation Warp Speed, and the Department of Defense's pandemic-influenced transition to telework.

For further details on those and other accomplishments, CISA encourages users and administrators to read the NSA Cybersecurity 2020 Year in Review.

Attackers Exploit Poor Cyber Hygiene to Compromise Cloud Security Environments

By CISA, Original release date: January 13, 2021

CISA is aware of several recent successful cyberattacks against various organizations' cloud services. Threat actors used a variety of tactics and techniques, including phishing and brute force logins, to attempt to exploit weaknesses in cloud security practices.

In response, CISA has released Analysis Report AR21-013A: Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services which provides technical details and indicators of compromise to help detect and respond to potential attacks.

CISA encourages users and administrators to review AR21-013A and apply the recommendations to strengthen cloud environment configurations.

With 2020 gone, what did the tech industry learn from COVID-19?

By Staff, Certification Magazine, Winter 2021

If the major theme of the last 20 years has been how information technology dramatically changed the world, then the year 2020 was when IT itself had to adapt, in order to serve a pandemic-stricken planet.

The COVID outbreak forced businesses, schools, healthcare providers, and governments to revisit their technology solutions to support a populace hampered by travel restrictions and disease control measures. Implementing these changes has taught the IT industry some critical lessons about what's required of technology during a global crisis.

What have we learned from coping with COVID? Let's take a look at some of the curveballs that came shooting at the IT industry this year and assess how they were handled. What IT norms were disrupted by the pandemic, and what COVID-related challenges is the IT industry likely to face in 2021?

COVID-19 reshuffles the deck

Arguably the biggest workplace technology issue to arise in 2020 was the immediate and pressing need to enable and advance the process of telecommuting. The mere thought of permitting people to work from home, to say nothing of helping them do it, is a contentious issue that has been hotly debated for years.

Spoiler alert: Work-from-home solutions? They work.

The COVID-19 outbreak forced the hand of nearly every organization that had previously refused to integrate WFH solutions into their enterprise. The persistent (and unfounded) prejudices against remote work were effectively discredited in 2020, as home-based information workers across multiple industries proved they can be effective, high-functioning, and fully engaged in their work … without being confined to a cubicle.

The sudden necessity of telecommuting, however, required IT departments to learn a tough lesson: Information security needs to be balanced with what WFH employees need access to in order to do their jobs.

Read the rest here:

http://certmag.com/2020-gone-tech-industry-learn-covid-19/

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

NIST Releases Supplemental Materials for SP 800-53 and SP 800-53B: Control Catalog and Control Baselines in Spreadsheet Format

By Staff, NIST, January 26, 2021

New and updated supplemental materials for NIST Special Publication (SP) 800-53, Revision 5, ***Security and Privacy Controls for Information Systems and Organizations***, and NIST SP 800-53B, ***Control Baselines for Information Systems and Organizations***, are available for download to support the December 10, 2020, errata release of SP 800-53 and SP 800-53B:

Control Catalog Spreadsheet **(NEW)** The entire security and privacy control catalog in spreadsheet format
Control Baselines Spreadsheet **(NEW)** The control baselines of SP 800-53B in spreadsheet format

Both spreadsheets have been preformatted for improved data visualization and allow for alternative views of the catalog and baselines. Users can also convert the contents to different data formats, including text only, comma-separated values (CSV), and other formats that can provide greater flexibility (e.g., by ingesting it into an existing product or platform and/or to facilitate automation). The spreadsheets were created from the Open Security Controls Assessment Language (OSCAL) version of the SP 800-53 Rev. 5 controls, which is offered as a supplemental material to the publications.

Additionally, the following existing supplemental materials for SP 800-53 were recently updated:

Analysis of updates between SP 800-53 Rev. 5 and Rev. 4 **(UPDATED)**

- **Mappings between SP 800-53 Rev. 5 and other frameworks and standards:**

  NIST Cybersecurity Framework and NIST Privacy Framework **(UPDATED)**

  ISO/IEC 27001 **(UPDATED)**

More information is available on the SP 800-53 publication page. Contact sec-cert@nist.gov with any questions and comments.

You might be an old government contractor if….

- You worked on something called “Star Wars” and it wasn’t the movie, but something Ronald Regan funded.
- You remember when DNA was short for Defense Nuclear Agency.
- You still have trouble saying NRO out loud because it was a classified agency when you first knew of it.
- People are declassifying documents now that you actually worked on.
- You remember when all computer networks only had dumb terminals.
- You remember a time before cell phones.
- The computers you learned to program with had 8” floppy disks.
- Your friends thought you worked with those small radio control airplanes called RC’S (RCS!).
- You used the Rainbow Series which isn’t something from the PBS series “Reading Rainbow”.
- Computer Security was alarming the room and spinning the combo lock.
- The Computer had its own *Room*.
- Data was stored on 8” floppy disks.
- Programs were loaded from punch cards.
- The customer tells you they don’t exist.
- IA inspections consisted of properly labeled systems.
- When our products were based on risk and not on check boxes.

- Servers so big they were on wheels now take up 2Us in a rack, and hold 100+ times the data.
- Equipment you once worked on is now in an exhibit in the Air Force museum (or the National Cryptologic Museum.)
- In networking, you actually know what the 3-4-5 rule is.
- Lotus 1-2-3, dBASE, Word Perfect, and Harvard Graphics were the standards for spreadsheets, databases, word processing, and presentations on many desktop computers.
- Your co-workers think Banyan Vines is a new candy.
- You mention Token Ring and people think you are getting married.
- Your co-workers think a boot infecting virus is some sort of foot fungus.
- You still say EPSQ occasionally.
- You say “Agency” when referring to any 3 letter agency because you can’t remember who is unacknowledged.
- When you hear the word “tapes” you don’t think about cassette tapes.
- You remember DITSCAP and complained of its beauracracy.
- You’ve read the REAL history of …things and places…
- If you talk about the Rainbow series and you end up in HR.
- If downloading a file required you to carry something.

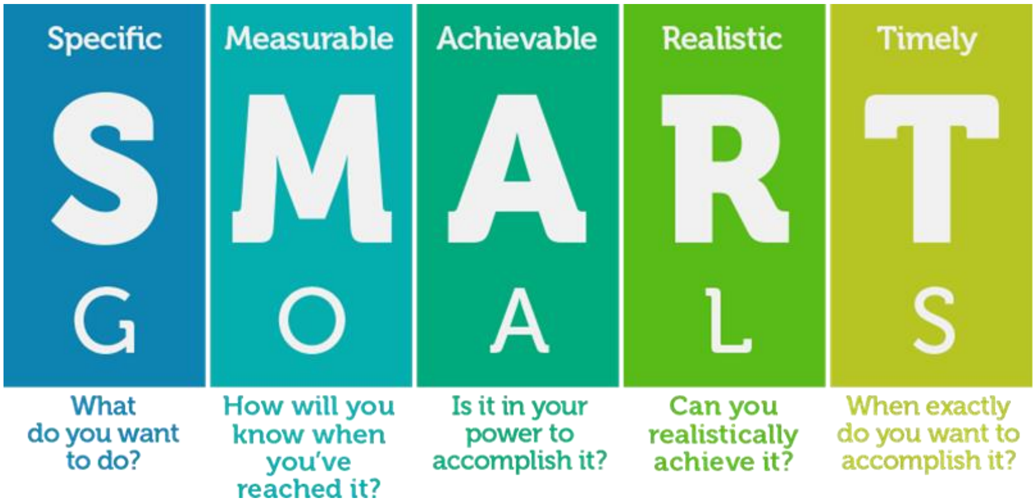
Mentoring Program

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.


Specific
S
G
What do you want to do?
Measurable
M
O
How will you know when you've reached it?
Achievable
A
A
Is it in your power to accomplish it?
Realistic
R
L
Can you realistically achieve it?
Timely
T
S
When exactly do you want to accomplish it?

Cyber Spotlight – PARTY!!

ISSA-COS turns 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**

Colorado Springs Chapter

WWW.ISSA-COS.ORG

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: Jeff Tomkiewicz
- Deputy: Phebe Swope

Member at Large 1: Art Cooper
Member at Large 2: Jim Blake
Member at Large 3: James Asimah
Member at Large 4: Jay Carson

Committee Chairs:

Annual Audit: Chris Edmondson
Training: Mark Heinrich
Mentorship Committee Chair: Carissa Nichols
Media/Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson
Girl Scouts Cyber Badge Camp: Anna Parrish
Annual Election: Colleen Murphy

**** Executive Board Members***

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

Past Senior Leadership

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

Iran 'hides spyware in wallpaper, restaurant and games apps'

By Gordon Corera, BBC, February 8, 2021

Iran is running two surveillance operations in cyber-space, targeting more than 1,000 dissidents, according to a leading cyber-security company.

The efforts were directed against individuals in Iran and 12 other countries, including the UK and US, Check Point said.

It said the two groups involved were using new techniques to install spyware on targets' PCs and mobile devices.

And this was then being used to steal call recordings and media files.

Read the rest here:

https://www.bbc.com/news/technology-55977537

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