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

ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 6 JUNE 2020

Welcome to June!

A Note From Our President

By Mr. Ernest Campos

Fellow Members of ISSA-COS,

Together, we have been through a lot these last few months but, thankfully society is beginning to slowly re-open. Hopefully, we will not encounter a second wave of the COVID-19 virus and we will be able to return to a more normal lifestyle soon. No doubt, our lives will be forever changed from this event and we should expect new social norms to become standard. Never-the-less, humanity is resilient, and we will learn to adjust and move forward.

Looking back at the month of May, we continued our online series with several great speakers and highly, engaging topics. Our series of online presentations have proven to be remarkably successful with strong registration and attendance records week after week. I hope many of you were able to join us and enjoyed the presentations we received from the following speakers: Ms. Jothi Dugar, Mr. Peter Sopczak, Mr. Trent Bunnell, Sr., Mr. Sean Deuby and Mr. Clark Brown from Semperis, Mr. Jay Carson, Ms. Erin Plemons, and Ms. Lori Hayes. Altogether, these knowledgeable and gifted speakers provided our chapter and our community with valuable information and technology updates regarding various aspects of our industry and our professional development.

Also launched in May was the Peak Cyber Symposium website (www.peakcyberco.com). Early bird registration is now open and offers FREE registration for all members of ISSA (regardless of their chapter affiliation), .mil, .gov, and .edu members of our community. Early bird registration will also gauge community interest and support for proceeding with an in-person conference. If state restricts don't allow or if community interest in supporting an in-person conference is low, we will need to shift to a virtual format. The best measure for this decision will be your early registration. Please support this event and communicate your support. Also available via the website is the Call for Speakers, Sponsors, and Exhibitors. Please spread the word to all your professional contacts and let them know Peak Cyber Symposium is OPEN!!

Looking forward to June, we will continue our online series with three more exciting presentations lined up. On June 4th, Checkmarx (www.checkmarx.com) will join

(Continued on page 4)

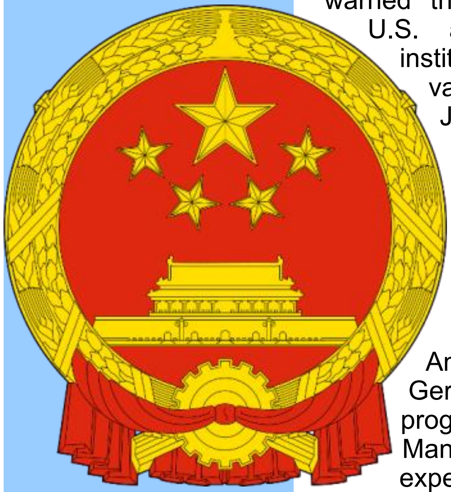
The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters .

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.

On Point: Communist China Continues to Target American Creativity

By Austin Bay, Strategy Page, May 13, 2020



In mid-April, a senior FBI official warned that cyber spies were attacking U.S. and allied medical research institutions developing coronavirus vaccines. The U.S. Department of Justice later pegged China as the chief witch doctor of medical espionage and suggested a crash American COVID-19/Wuhan virus vaccine project nicknamed Operation Warp Speed is Beijing's major target.

During World War II, American leaders feared Nazi Germany sought a nuclear weapons program. So at warp speed, the Manhattan Project split atoms in an experimental reactor and then developed and deployed operational atomic bombs.

The "crash" Manhattan Project gave the U.S. and its allies a decisive strategic-warfare edge. A-bombs ended the conflict and saved lives by avoiding a bloody, Okinawa-type invasion of Japan.

My opinion: Nuclear proliferation remains the sane world's major security threat. However, the COVID-19/Wuhan virus' global proliferation (attention: it originated in Wuhan) has demonstrated (once again) that pandemics are an international security threat to human life. They also savage 21st-century economies.

“Who do the authors seek to defeat? The U.S.A.”

That means the nation that develops and deploys the first safe and clinically effective vaccine will be able to do many things. Protecting your nation's population is more than a material medical advantage. A vaccinated population has an economic advantage over adversaries.

Developing an effective vaccine enhances diplomatic power. Obviously, the discoverer's allies are in line to benefit. But don't underestimate prestige power of an effective vaccine's quick discovery and rapid employment. Effectiveness is primary. However, speed demonstrates a society's ability to rapidly face new, threatening conditions and produce a response that benefits the world.

A Nobel Prize isn't the only measure of a nation's creative scientific vitality, but it is a measure even television gab shows understand. Hence this column's side bet: An effective COVID-19/Wuhan virus vaccine developed by fall 2020 will warrant a Nobel Prize in Medicine.

I repeat from last week's column, for the sake of Chinese communist propagandist idiots, that Wuhan is a place, just like the Rocky Mountains (Rocky Mountain spotted fever), Uganda's West Nile province (West Nile virus), Old Lyme, Connecticut (Lyme disease), and Congo's Ebola River (Ebola virus).

Why hammer that fact? Because attempting to disconnect the virus from its country of origin -- China -- is a Chinese Communist Party propaganda ploy to shield CCP leaders from taking responsibility for having spread the virus.

The agitprop campaign has failed. In fact, the pandemic has focused attention on communist China's global depredations and in particular its "unrestricted warfare" attack on the U.S.

"Unrestricted Warfare" (also known as "Warfare Without Limits") is the title of a book authored by two People's Liberation Army Air Force colonels. Published in 1999, the colonels propose weakening and then defeating an adversary using an array of operations -- for example, theft, bribery, economic gimmicks, disinformation, spying, co-optation of an adversary's media and educational institutions.

In May 2019, I wrote a column noting spies have always sought more than military secrets. Gathering political intelligence and economic information aren't new, though global competition has enhanced the value of "proprietary knowledge," particularly when the intellectual property involves technology or techniques with national security application.

Read the rest here:

https://strategypage.com/on_point/202005139403.aspx

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.

New Members May
Cecil Wilkinson
Dr. Ronald Davis
Daniel Pocius
Eric Thompson
Robert William Benjamin

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

Our membership is hanging in at ~351 members as of the end of May 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

CISA-FBI Joint Announcement on PRC Targeting of COVID-19 Research Organizations

Original release date: May 13, 2020

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have jointly released a Public Service Announcement on the People's Republic of China's targeting of COVID-19 research organizations. CISA and FBI encourage COVID-19 research organizations to review and apply the announcement's recommended mitigations to prevent surreptitious review or theft of COVID-19-related material.

For more information on Chinese malicious cyber activity, see https://www.us-cert.gov/china.

This product is provided subject to this Notification and this Privacy & Use policy.

(Continued from page 1)

A Note From Our President

us as a Single Event Sponsor and guest speaker, Mr. Peter Archibald. On June 11th our very own former VP of Training, Mr. Jeff Tomkiewicz will guide us through a Capture-the-Flag (CTF) experience via the TryHackMe website. Later in the month on June 25th, we will showcase our new strategic partnership with Info-Tech Research Group. On that evening, Ms. Nina Di Francisco will provide a benefits overview for our chapter members and invite one of her industry analysts to provide a topical presentation. Please register early for this event as a minimal amount of setup time will be required.

Looking further down the road, ISSA-COS is bracing for the potential of having to maintain a virtual format for all our monthly events through the end of 2020. Since we rely on the generosity of other organizations with physical meeting spaces, these organization might not open to outside groups such as our chapter until 2021. If that proves to be the case, rest assured our chapter will continue to schedule high quality online presentations for as long as necessary.

In closing, I remain proud of the many volunteers our chapter has helping to keep our mission moving forward. From our IT Committee, Speakers Bureau, Key Personnel, and Board of Directors, our chapter is one of the strongest chapters in the state, in our nation, and across the globe. Thank you to everyone to supports us with your time, re-posts our social media announcements, and educates other about our chapter simply by word of mouth. Together, our chapter and our community work together for the betterment of everyone in it.

Sincerely,

Ernest

CISA, DOE, and UK's NCSC Issue Guidance on Protecting Industrial Control Systems

Original release date: May 22, 2020

The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE), and the UK's National Cyber Security Centre (NCSC) have released Cybersecurity Best Practices for Industrial Control Systems, an infographic providing recommended cybersecurity practices for industrial control systems (ICS). The two-page infographic summarizes common ICS risk considerations, short- and long-term cybersecurity event impacts, best practices to defend ICS processes, and highlights NCSC's product on Secure Design Principles and Operational Technology.

CISA, DOE, and NCSC encourage users to review Cybersecurity Best Practices for Industrial Control Systems. For more in-depth information, visit CISA's ICS Recommended Practices webpage and DOE's [https://www.us-cert.gov%20https:/www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0]Cybersecurity Capability Maturity Model (C2M2) Program webpage. For information on CISA Assessments, visit https://www.cisa.gov/cyber-resource-hub.

This product is provided subject to this Notification and this Privacy & Use policy.

Cyber security and space security

By Nayef Al-Rodhan, The Space Review, May 26, 2020

In 2014, the network of the National Oceanic and Atmospheric Administration (NOAA) was hacked by China. This event disrupted weather information and impacted stakeholders worldwide. Satellites are often highly vulnerable to cybersecurity breaches as some telemetry links are not even encrypted.

Cybersecurity is defined by the International Telecommunication Unionas "the collection of tools, policies, security concepts… risk management approaches… and technologies that can be used to protect the cyber environment and organization." Space security can be understood similarly, but instead towards the protection of outer space and assets there. This article aims at understanding the links between these two notions and the challenges at their junction.

Two intertwined domains

My theory of meta-geopolitics outlines seven interrelated dimensions of state power (social and health issues, domestic politics, economics, environment, science and human potential, military and security issues, international diplomacy) that constitute the new paradigm of statecraft. The book *Meta-Geopolitics of Outer Space explains* how these seven dimensions are present in outer space. In the social and health sector for instance, satellites are crucial to monitor diseases or even guide remote medication delivery systems. In the case of the COVID-19 outbreak in China, it appeared that disease monitoring and large scale disinfection by unmanned aerial vehicles, guided by 28 BeiDou Phase III navigation satellites, were crucial to mitigate the spread.

Space is thus a critical asset for the modern state and the challenges it faces. This dependency relies on the critical interaction of cybersecurity and space security. Indeed, several data flows can be identified between the Earth and space-based assets. First, information is sent from Earth to satellites and other space-based assets (Earth-space interactions.) Second, information is sent back to Earth from satellites and other space-based assets (space-Earth interactions.) These flows are critical and vulnerable to threats. The security of space-based infrastructure depends on the safety of Earth-space interactions, and the security of systems relying on data from space depends on the safety of space-Earth interactions. For example, false information could be given by Earth-based attackers to a satellite to force it to collide with another.

New dynamics in outer space have increased the level of vulnerability of cyberspace and space-based infrastructures. Indeed, space used to be reserved to major powers as the expertise and technologies required were scarce. However, innovations such as cubesats and the privatization of outer space made access to space easier and cheaper. New states and individuals have access to this domain and multiply the presence in the LEO, and thus the risk of malicious interactions. Moreover, growing space militarization may increase the risks of confrontation and thus the numbers of attacks.

On Earth, the increased number of self-trained or state-supported hackers, as well as the cheap access to computer technologies, also increases the risk of disruption to Earth-space and space-Earth interactions. These attacks are particularly hard to trace and thus complicate the attributions of responsibilities.

Threats at the junction of space and cyber security can be placed in five categories: kinetic physical, non-kinetic physical, electronic, cyber, and Earth-based. Kinetic physical threats include direct strikes against space infrastructure, either through another satellite or a weapon such as anti-satellite systems (ASATs.) Non-kinetic physical threats damage space assets through effects from a distance, such as electromagnetic pulses (EMP). Hackers could take control of such systems to launch attacks. With the rise in innovative processes, electronic and cyber threats are however more widely used. Electronic threats include actions undertaken to damage the transmission and reception of data (jamming) or even the transmission of false data (spoofing.) Cyberattacks in this domain mostly deal with the direct injection of false data or the unauthorized monitoring of traffic or activities in outer space. Finally, Earth-based threats include the malicious acts within the supply chains of these systems or against the physical infrastructures used for transmission or storage of data. To be mitigated, all these potential threats require international cooperation, a process that for the time being seems quite stuck.

National capabilities

The United States' space operations are advanced but vulnerable. Additionally, the United States itself has the capabilities to conduct kinetic physical, kinetic non-physical, electronic, and cyber attacks. It is, however, hard to precisely measure the capability of the United States as most information in this domain is classified. The activities of the Space Force, for example, are not actively shared. In terms of cyberattacks capacity we can however note that the National Security Agency has recently declared its willingness to use cubesats for better intelligence collection and vulnerabilities assessments. It thus appears that the United States has significant resources but keeps communication on this matter low key.

Read the rest here:

https://www.thespacereview.com/article/3950/1

The New Guy's View of Cybersecurity

By Jay Carson, ISSA-COS member, May 7, 2020. Jay can be reached at runningjay51@gmail.com, and would appreciate your comments or criticisms.

Two past ISSA-COS presidents suggested I write an article on my observations of the cybersecurity field, as a newcomer. I am a (retired) senior Air Force civil engineer, with 30+ years of experience as active duty military, a contractor, and civil service. Over the years I was involved in a wide variety of the construction disciplines, everything from utilities to structural projects to pavement.

I got into cybersecurity in the last three years, so far reading 20+ cybersecurity books, getting my Security+ and Certified Information Privacy Professional / Europe certifications, and being active in ISSA-COS. It has been an interesting experience seeing how a (relatively) new profession has evolved, with all its growing pains. So how do I think cybersecurity is different, and how is it like civil engineering? In my opinion:

The first difference: *In terms of how cybersecurity pros acquire wisdom, you are somewhat the inverse of civil engineering.*

In civil engineering, if we could bring to life an engineer of the pyramids and make him a guest speaker at a professional association banquet, it would be standing room only! The profession has been around several thousand years, and while techniques and some materials have improved greatly, the basics (we move heavy things) have not changed all that much. Training and education from decades past is still relevant.

In cybersecurity, currency (or more properly, a youthful hunger for more knowledge) seems to be everything! Years of experience do matter, but cybersecurity professionals seem to need a young attitude to be successful. Is the factual knowledge gained in a 20 year old computer science degree really useful to you? Or is continuing education to keep up your certifications more relevant?

The second difference: *The traditions of office appropriateness are less relevant!*

Even though civil engineering types spend a lot of time on construction sites, they start at dawn and wear their mud with distinction. There is also a lot of 'business attire' time.

In cybersecurity, it seems to me that young person in the whoop-de-do T-shirt and sandals who makes it to the office at the crack of noon may be the most brilliant, productive team member. They may well provide spot-on results at 3:00 AM the next morning. Often cybersecurity types seem to care little for appearance - only results matter. If you are a cybersecurity 'boss,' I don't think you will get the best people if you rely too much on traditional office workplace standards.

That said, reliability seems to play heavily in both fields. Can you count on that person to deliver on time, or at least tell you ahead of time if they cannot?

The first similarity: *Cybersecurity has folk wisdoms just like civil engineering!*

In civil engineering, a folk wisdom is "water runs downhill." Everybody knows that, right? Well everyone may know that, but civil engineering types often do not act like they know that. Ever slip on a cake of ice in a parking lot? Likely either the designer or the constructor did not ensure proper drainage.

In cybersecurity, I don't yet know all your folk wisdoms, but assume one is similar to "You cannot eliminate risk, only lower it today. Tomorrow you need something better." What other folk wisdoms do you have? For example, a reviewer of this article said another wisdom is "In cybersecurity, the only constant is change." Another gave me their favorites in a series (I don't know any of the original sources despite a due diligence search, so please forgive me for the lack of citations.):

- “It’s not if you are going to be hacked, but when.” - Incident Response.
- “Well I never saw that error before...” - 0400 hours, Web Application Test.
- “Wait!!! I just started...” - 45 Hours into a 20 Hour Network Test.

(Continued on page 7)

(Continued from page 6)

- “Syntax is cruel” - Anyone writing or debugging code.
- “Methodology always counts more than the tool” - the OSINT analyst

Still another reviewer said:

- “The laws of physics do not change."
- "60 hertz/cycles does not change.”

What are your favorites to add?

The second similarity: *There is an astonishing lack of appreciation and knowledge in the lay public about the civil engineering and cybersecurity professions!*

Regarding civil engineering, there are people still out there thinking concrete 'dries,' and the faster you get it dry the sooner it reaches full strength. Actually, concrete cures in a chemical reaction, and you want to keep it reasonably warm and damp, certainly at the start. It won't reach 100% strength for a month or more.

As silly as this sounds, in cybersecurity I am told if we turned over every workplace keyboard in the US, we would still find a few instances of taped passwords. Keep your outreach education programs going, folks, and pay attention to your relatives' cybersecurity. Does your Mom practice good cybersecurity, based on what she does online? Would it bother you if you did not try to protect your mom, and she was cyber-hurt?

The third similarity: *Paranoia is your best friend!*

Civil engineering types are uneasy around the weather gods. Mother Nature is all powerful! In civil engineering you can influence Mother Nature's way of achieving her desires, but for the last couple of thousand years every time civil engineering stands against her, we lose.

Cybersecurity types seem to be uneasy regarding the unknown hacker. Again I am told just because you can't yet detect them, doesn't mean they are not out there stalking you.

To stay healthy, both professions seem to need to stay alert. By the way, there is a terrific book they had us read on this subject before I deployed to Afghanistan:

DeBecker, Gavin. *The Gift of Fear*. New York: Random House, 1997.

The author claims the things that make your nose twitch are subconscious signals designed to keep you alive and healthy. He says we ignore them at our peril.

The fourth similarity: *Knowing jargon does not necessarily mean possessing useful knowledge!*

Many people know, and throw around, civil engineering terms. They may not know what they mean in context, but they think it makes them sound cool. You cybersecurity professionals definitely have your own very cool language of acronyms and slang, but does that always equate to knowledge? I also wonder if you are finding some cybersecurity practitioners know the surface 'what,' but not the in-depth 'why.' I am curious, and I am interested in what you are finding.

I am very happy to be a new member of the cybersecurity community, especially the privacy portion. Protecting individual privacy is a certainly an honorable, if not noble, pursuit! Has everyone read Justice Louis Brandeis and Samuel Warren's work "The Right to Privacy," (Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890)? Good on you, cyber-sheep dogs of the world!

The author thanks the following ISSA-COS reviewers (alphabetical order): 'Coop' Cooper, Wally Magda, Mark Spencer, Colleen Murphy, and Justin Whitehead.

Responsibilities for opinions, or errors in fact are my own.

ISSA Fellow Program

2020 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 400 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the Fellow Program, once the 2020 award criteria is made available please contact Colleen Murphy at past-president@issa-cos.org to help you through the steps. Below are some details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. Applications will be accepted in the near future, and details will be provided in a future newsletter. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2020 ISSA International Conference.

To Become a Senior Member

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

Senior Member Qualifications

- 5 years of ISSA membership
- 10 years relevant professional experience
- For your convenience, we will have available the Senior Member Application Check-list to confirm eligibility and completion of application

All Senior Member applications require an endorsement from their home chapter to qualify.

To Become a Fellow or Distinguished Fellow

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow.

Fellow Qualifications

- 8 years of association membership.
- 3 years of volunteer leadership in the association.
- 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty developing and teaching courses.

All Fellow applications require a nomination to qualify.

Distinguished Fellow Qualifications

- 12 years association membership.
- 5 years of sustained volunteer leadership in the association.
- 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability.

All Distinguished Fellow applications require a nomination to qualify.

https://458rl1jp.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.issa.org%2Ffellows-program%2F/1/01000171dcdf328e-1f321b60-127b-44e5-a53d-39fa514c70c5-000000/_QtQ0l9nkskTqK4YDIJgaD08HQQ=160

2020 ISSA Awards Program

We are continually monitoring and making the best decisions we can, based on the health and welfare of our members, our staff, and our community at large. Given the nature and uncertainties surrounding this pandemic, we have decided to move our annual awards ceremony and dinner to a new date in the fall. The new date and details will be published as soon as we have confirmed our plans.

In this spirit we have decided to extend the ISSA Awards and ISSA Fellows Program nomination and entry deadline to July 25, 2020.

NOMINATE NOW!

As cyber security professionals your voices and opinions are the most valuable when it comes to providing awareness of peers and organizations in our communities doing incredible work to propel our industry forward. *They deserve to be noticed* so please honor them with a nomination to one of the following awards:

- Hall of fame
- Honor Role
- Chapter of the Year
- Volunteer of the Year
- Organization of the Year
- Presidents Award for Public Service
- Security Professional of the Year

For details on each category and to nominate **click here**

The ISSA Fellows Program honors established cyber professionals with demonstrated success and contributions to the industry. These individuals have dedicated years towards the innovation and progression within the cyber realm.

For more details and to nominate a notable individual please **click here:**

We appreciate your participation and time in helping to recognize our shining stars in the community.

Thank you.
Marc Thompson
Executive Director
ISSA International

How two researchers used an app store to demonstrate hacks on a factory

By Sean Lyngaas, CyberScoop, May 12, 2020

When malicious code spread through the networks of Rheinmetall Automotive last year, it disrupted the German manufacturing firm's plants on two continents, temporarily costing up to $4 million each week.

The attacks were the latest reminder to factory owners that computer viruses can hobble production. While awareness of the threats has grown, there's still a risk that too many organizations view such attacks as isolated incidents, rather than the work of a determined attacker that could be visited upon them.

Federico Maggi, a senior researcher at cybersecurity company Trend Micro, set out to dispel that mindset. So he used a laboratory housed at Politecnico di Milano School of Management, Italy's largest technical university, to show how attackers could disrupt production on the factory floor. His goal was to use the hypothetical hacks to help organizations address weaknesses in their defenses before actual attackers strike.

"We wanted to look for something different, something that future attackers may want to use," Maggi told CyberScoop.

Maggi and Marcello Pogliani, a colleague from the university, produced a 60-page study detailing different ways of attacking a factory to make their point: It's not about one vulnerability or one system. A determined hacker could have a range of options for slipping their disruptive code into a facility.

For instance, the researchers demonstrated a hack of machinery used to drill holes in toy cell phones, and showed how a supply-chain attack could distort temperature readings in the factory, bringing it to a halt. They used software libraries to deliver malware to factory devices that interact with those software tools.

Maggi started with a popular application marketplace maintained by Swiss industrial giant ABB that engineers use to upload programming code for factory robots. He found a vulnerability in the app store that let him upload his own code to the store. Once that code was installed at an engineering workstation on his factory floor, Maggi said, he was able to harvest data from the workstation.

"There was no sandboxing," Maggi said. "We were able to read files, exfiltrate files from that machine just with a simple plugin."

ABB ultimately fixed the vulnerability.

The research comes with important caveats: Maggi was not attacking a factory staffed with people who might be able to detect the attacks, which involved breaking into different machines in stages. And some of the attacks required access to a network to execute.

Evil twins

Maggi also took aim at the "digital twin," a digitized replica of a factory machine or process that manufacturers use to test performance. He uncovered a flaw in software that manages digital twins and showed how an attacker might manipulate the code. The factory's machinery could, in theory, be tricked into producing goods based on the faulty design.

The issue is larger than that. With mobile phone apps, for example, the Android or iPhone downloading them have a standard way of verifying that they're legitimate and not pirated. But with digital twins, Maggi said, that's not the case.

"There's no standardized way to communicate and to transfer digital twins in a way that there is full integrity checks applied at every step," he said.

His paper makes several security recommendations for mitigating the attacks, including validating software deployed on workstations. But some of the supply chain issues the paper raises will take longer to address.

Read the rest here:

https://www.cyberscoop.com/trend-micro-factory-attacks-federico-maggi/

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)

Peak Cyber Symposium – *10th Anniversary!*

The Peak Cyber Symposium is an annual 3-day event that attracts over 500 attendees from across the nation. This event kicks off with a full day of Capture-the-Flag (CTF) fun and competition. A morning CTF prep session for beginners followed by the actual competition in the afternoon. Lunch is provided and snacks are served throughout the day.

The following 2-days include a series of keynote speakers, panel discussions, breakout sessions, and an exhibitor hall. Community representatives from partnering organizations are on hand to educate and inform attendees on events coming up within the community. Each annual Peak Cyber Symposium emphasizes an industry relevant theme.

Sept. 15-17, 2020
DoubleTree Hotel
Register at:
www.issa-cos.org
info@issa-cos.org

Highlights for this event include:

- Nationally recognized Keynote Speakers and Fortune 500 Sponsors/Exhibitors
- Up to 24 potential Continuing Professional Educations (CPE) Credits Available
- Over 100 Capture-the-Flag participants - all skill levels are welcome – *beginners too!*
- Over $10,000 in prizes and giveaways
- Networking, Networking, Networking!!
- 40 Exhibitor Booths with Live Demos
- Free parking, Free breakfast, Free afternoon snacks.

Strategic Partnership: Info-Tech Research Group

- ⇒ Peer Benchmarking
- ⇒ Quarterly research content
- ⇒ Personal concierge/support for key IT challenges
- ⇒ Co-branded landing page for ISSA-COS members
- ⇒ Access to 250+ Analysts/VPs to serve as mentors, research analysts, and guest speakers

INFO~TECH
RESEARCH GROUP

2020 CISSP Online Review

<u>June Schedule– 6 Sessions</u>

Fri—6/5 (2-6 PM)

Sat—6/6 (8-4 PM)

Sat—6/13 (8—4PM)

Fri—6/19 (2-6 PM)

Sat—6/20 (8-4 PM

Sat—6/27 (8-4 PM)

Member Fee: ~~$200~~ **Now $100**

Non-Member Fee: ~~$600~~ **Now $300**

Register at: www.issa-cos.org

June/July Online Series

<u>06/04/2020 / Session 1</u> **Paid Sponsor:** Checkmarx

Speaker: Mr. Peter Archibald, *(ft. Mr. Jeff Hsiao, Mr. Michael Lee, and Mr. Jeffrey Armstrong)*

Topic: The Application Security Journey

<u>06/11/2020 / Session 2</u>

Speaker: Mr. Jeff Tomkiewicz, *Former ISSA-COS Deputy VP of Training*

Topic: Hands on Capture-the-Flag (CTF) using the TryHackMe website

<u>06/25/2020 / Session 3</u> **Strategic Partner:** INFO~TECH RESEARCH GROUP

Speaker: Ms. Nina Di Francisco, *Director, Info-Tech Research Group*

Topic: Info-Tech Research Group Overview

<u>07/09/2020 / Session 1</u>

Speakers: Mr. Frank Gearhart, *C|CISO, CISSP, C|HFI, C|ND, ISSA-COS Past President*

Topic: Quantum Cryptology and How it Impacts our Profession

<u>07/23/2020 / Session 2</u>

Speaker: This could be *<u>YOU!</u>*

Topic: TBD

Register at: www.issa-cos.org or

to become a guest speaker, email: SpeakersBureau@issa-cos.org

Senator Pushes to Require National Cyber Director in Defense Authorization Bill

By Mariam Baksh, NextGov, May 13,2020

The head of the Senate Homeland Security and Governmental Affairs Committee wants to require a Senate-confirmed national cyber director in the coming annual defense authorization bill.

“The first recommendation I want to talk about which we’re working hard to get hopefully included in the defense authorization act so it can become law, is the need to put somebody in charge, a national cyber director,” Chairman Ron Johnson, R-Wis., said.

Johnson was referring to recommendations of the National Cyberspace Solarium Commission, members of which testified Wednesday during a committee hearing.

Johnson also pushed and heard support for legislation he’s proposed with Sen. Maggie Hassan, D-N.H., which would give the Cybersecurity and Infrastructure Security Agency subpoena power over internet service providers, to be included in the NDAA.

Rep. Mike Gallagher, R-Wis., a co-chair of the commission, explained how a new cyber director’s office would differ from CISA.

“CISA is always primarily going to have that mission of defending critical infrastructure, the .gov space, in a similar way in which [the National Security Agency] and [U.S. Cyber Command] defend the .mil space,” he told the committee. “The national cyber director would have a more coordinating function that is making sure that CISA, in performing that mission is also working well with NSA, with Cybercom, and all the other federal agencies that play in the cyber space.”

The would-be cyber director’s office would be able to coordinate across missions and do long term planning as CISA fights on a day-to-day basis to protect civilian agencies, he said.

Solarium commission member Suzanne Spaulding, who previously led the Department of Homeland Security Office that became CISA and served as general counsel to the Central Intelligence Agency, added the director would be able to bring together offensive and defensive planning. Such a director also could incorporate authorities of the intelligence services and the military into a broader effort to protect the U.S. from cyber threats.

The idea of a national cyber coordinator is not new. Former National Security Advisor John Bolton eliminated a similar post in May 2018, saying it amounted to unnecessary bureaucracy within the National Security Council.

Gallagher said the commission’s recommendation is for the cyber director’s office to be modeled off that of the U.S. Trade Representative “because it’s interdisciplinary, it’s functionally oriented, and it’s institutionalized with Senate-confirmed leadership and situated within the executive office of the president.”

Johnson said he signed onto a letter with Sen. Mike Rounds, R-S.D., chairman of the Senate Armed Services’ subcommittee on cybersecurity, asking Sen. Angus King, I-Maine, to lay out more of such details on what the cyber director’s position would look like so it can be included in the NDAA.

Read the rest here:

https://www.nextgov.com/cybersecurity/2020/05/senator-pushes-require-national-cyber-director-defense-authorization-bill/165374/

IoT security: How these unusual attacks could undermine industrial systems

By Danny Palmer, ZDNet, May 12, 2020

Hackers could target smart manufacturing and other industrial environments with new and unconventional cyberattacks designed to exploit vulnerabilities in ecosystems that are supporting the Industrial Internet of Things (IIoT), according to academics and security company researchers.

Researchers at cybersecurity company Trend Micro and experts at the the Polytechnic University of Milan examined how hackers can exploit security flaws in IIoT equipment to break into networks as a gateway for deploying malware, conducting espionage or even conducting sabotage.

While these networks are supposed to be isolated, often there can be links with the general office systems across an organisation, especially if there isn't segmentation on the network.

Putting smart manufacturing systems on their own dedicated network is common practice, as is treating them 'like black boxes' said the report, in the sense that it is assumes that nobody will ever be able to compromise them. However, increasingly vendors are pushing for wireless networks on the factory floor, with things such as industrial robots directly connected to them.

Performing tests against real industrial equipment in the safety of the University of Milan's Industry 4.0 lab, researchers uncovered a number of ways attackers could exploit vulnerabilities to gain access to smart manufacturing environments.

One example of this came when it was discovered there were vulnerabilities in a particular application that is used to help design and build robots and other autonomous systems, enabling attackers with access to the development network to install unverified add-ins.

These could be used to monitor the entire development process – and providing the attackers with the means to gain access to and control the network that a smart device is run on, jumping from the device to other systems and a potential means of espionage.

Fortunately, researchers have already been in touch with the application providers behind the software vulnerabilities that were found – and this particular loophole has been closed.

But that wasn't the only method researchers found they could exploit to gain access to smart networks by modifying an IIoT device to such an extent they can exploit it to control or modify how an operational environment works. Attackers would likely gain access to it via a vulnerability in the software supply chain of the device, perhaps in the method described above.

This is particularly concerning when it comes to sensors and monitoring systems, which depending on the circumstances can do everything from providing alerts on when maintenance is needed, to actively controlling anything from the temperature of an environment to physical systems.

But with access to such systems, an attacker could alter readings on the network, so as to not give away that any suspicious activity is happening, even if they are making adjustments to functionality.

Alternatively, attackers could be much much less subtle, either by using a network of trojanized devices to take down a network in a DDoS attack, or by controlling devices that set off alarms or do other highly noticeable activities. Other potential ways onto these networks include compromised workstations or the app stores that are now being developed to offer add-ons for industrial systems.

All of these scenarios serve as an active reminder that if not properly managed, cyber-physical systems can be compromised and exploited in a variety of ways.

Read the rest here:

https://www.zdnet.com/article/iot-security-how-these-unusual-attacks-could-undermine-industrial-systems/

Notes from the ISSA-COS Speakers Bureau

By Jay Carson, ISSA-COS Speakers Bureau

As you know, the ISSA-COS team has been successful at providing an online program of speakers to the chapter in lieu of the Cyber Focus Day(s), in-person chapter meetings and mini-seminars. Through the May 28th offering, we have been able to offer members approximately 55% of the continuing education credits they could have received had the in-person events taken place. Not too bad!

President Ernest Campos, on behalf of the chapter, has thanked all the speakers and ISSA-COS team members who made this possible.

Normally, after in-person presentations attendees are able to exchange business cards for networking. We want to match that offering as much as possible with our online program. The purpose of this article is to summarize the presentations thus far (each synopsis provided by the presenters) and give contact information if ISSA-COS members wish further contact with the speakers.

April

1. 2 April 2020: **Speaker:** Mr. Art Cooper, ISSA-COS Member-at-Large. **Topic:** A discussion on the "Challenges" of working from home and remaining "Secure." **Synopsis:** Thanks to the Coronavirus crisis, organizations are now scrambling to enable their employees to work from home. This is presenting a whole new series of challenges to compliance, technology and information security teams as these employees are now operating in a potentially less secure and definitely less private environment. Every home network environment is different and could pose significant security challenges. Mr. Cooper discussed how best to work from home while remaining secure. **Contact:** Mr. Cooper can be reached at artcoo1961@gmail.com.

2. 9 April 2020: **Speaker:** Mr. Wally Magda, CEO | Owner WallyDotBiz LLC. **Topic:** How do you keep the lights on and the gears turning during a global pandemic? **Synopsis:** ICS/SCADA critical infrastructure is "insecure by design." It was designed to work; it was not designed to be secure!! In addition to threat actors, ransomware and bots, what is the impact of pandemic stress on your systems? What about your supply chain? What is your resilience against disruption to the availability of critical components, materials, and support resources with supply chains originating in or traversing significantly impacted regions globally? What about your people? Remote access plays a key part in keeping the gears turning and keeping the lights on. However, even with all the automation, remote control can only go so far. Oh my!!! You just learned that a cryptographic key utilized to protect the account password is hard coded into the programs running on your control devices. An attacker can easily use that information to launch ransomware and bring you down. The vulnerability rating severity is a 10-CRITICAL. You can't patch that remotely! Now what do you do? **Contact:** Mr. Magda can be reached at wladekco@comcast.net.

3. 16 April 2020: **Speaker:** Dr. Erik Huffman, CEO/Founder, Handshake Leadership. **Topic:** Psybersecurity (No typo). **Synopsis:** Cybersecurity is the combination of technology, organizational operations, people, and culture. This talk specifically address issues residing in the sociological impacts in cybersecurity. Dr. Huffman is a cybersecurity researcher in the emerging field of cyberpsychology; the combination of cybersecurity and psychology. His research has led him into the exploration of the effectiveness of cybersecurity training. It has been said that we need to train how we fight. What happens when we actually do that? **Contact:** Dr. Huffman can be reached at erik.huffman@handshakeleadership.com.

4. 23 April 2020: **Speakers:** ISSA-COS Members Mark Spencer (ISSA-COS President Emeritus), Justin Whitehead (Digital Silence), Rob Carson (Semper Sec), Jay Carson (ISSA-COS Speakers Bureau). **Topic:** In the Time of Pandemic, are Written Cybersecurity Policies and Procedures Less Important, or More? **Synopsis:** Work-from-home requirements are creating more targets for cybercriminals. Should companies' written policies and procedures be updated and reinforced to meet a greater threat? For the first 30 minutes, Justin Whitehead and Rob Carson will answer questions from Jay Carson about the latest tactics of cybercriminals. Are spear-fishing and whaling still valid threats, or are all the important targets cyber-safe? For the last half of the program, Mark Spencer will give ways to hinder the latest tactics of criminals with his perspective on written cybersecurity policies and procedures. Are the old lessons more, or less important in this changing time? **Contacts:** Mr. Spencer can be reached at mark.l.spencer@comcast.net.

(Continued on page 17)

(Continued from page 16)

Mr. Whitehead can be reached at whitehead@digitalsilence.com. Mr. Rob Carson can be reached at rob.carson@sempersec.com. Mr. Jay Carson can be reached at jay@sempersec.com.

5. 30 April 2020: **Speaker:** Ryan Dozier, Security+, Network+, Cybersecurity Systems Engineer Manager, ManTech. **Topic:** Cybersecurity Strategy. **Synopsis:** Building a high-level cybersecurity strategy that shows what your system/program/business is doing for Cybersecurity. Mr. Dozier discussed what impacts there are to your program, what requirements you need to apply, what your budget is, how you apply risk to your system/program, timelines, approaches, and key roles. **Contact:** Mr. Dozier can be reached at rdozier22@gmail.com.

May

1. 7 May 2020: **Speaker:** Ms. Jothi Dugar, CISO, Author, Public Speaker, Wellness Expert & Practitioner. **Topic:** The Holistic & Integrative Approach to Cyber Risk Management. **Synopsis:** The world of cyber is changing rapidly each day. Cyber professionals and leaders must learn to adjust to this rapidly growing field by looking Cyber Risk Management through a holistic and integrative approach. Concepts such as cyber governance and leadership, diversity, incident response, and the role that mental health & wellness will be explored using a holistic and integrative approach. **Contact:** Ms. Dugar can be reached at jothi.dugar@gmail.com.

2. 14 May 2020: **Speakers:** Peter Sopczak, CEH. Information System Security Manager at Pluribus International. Trent Bunnell, Sr., Security+. Information System Security Officer at LinQuest. **Topics:** Mr. Sopczak - Incident Response. Mr. Bunnell - Risk Management Framework. **Synopsis:** Mr. Sopczak - Common mistakes and how to make the plan more effective. Mr. Bunnell - How the Risk Management Framework is utilized to keep government systems secure. **Contacts:** Mr. Sopczak can be reached at pjsopczak@gmail.com. Mr. Bunnell can be reached at https://linkedin.com/in/trent-bunnell.

3. 21 May 2020: **Speaker:** Sean Deuby, Director of Services, Semperis and Clark Brown, Partner and Practice Leader, Alescent. **Topic:** Ransomware vs. Active Directory Backups: What Can Throw a Wrench into Your Disaster Recovery Process? **Synopsis:** In a cyber disaster, you must recover Active Directory before you can recover your business. But only one in five organizations have a tested plan in place for recovering AD after a cyberattack. This is alarming given the spike of ransomware attacks and the widespread impact of an AD outage. Organizations must now be able to quickly recover their AD domain controllers and protect against rogue scripts. However, traditional backup methods don't always address ransomware scenarios. Considering that cyber disasters now strike more frequently and inflict more business damage than natural disasters, it's time to think "cyber-first". Cyber-first requirements for AD recovery:

- Fully automate AD forest recovery
- Prevent malware re-infection from BMR and system state backups
- Restore AD to any hardware (virtual or physical)
- Regain control of a compromised AD
- Ensure the integrity of highly sensitive AD forests

Contacts: Mr. Deuby can be contacted at seand@semperis.com. Mr. Brown can be contacted at Clark.Brown@Alescent.com.

4. 28 May 2020: **Speaker:** Erin Plemons, CEH, Certified Hacking Forensics Investigator, Security +, Linux+, Information Systems Security Engineer at ENESCO, Inc. and Lori Hayes, B.Ch.E., CISSP, SH301, DSH301, DIBNET, ICSJWG, A+, Network+, MCSA, Critical Infrastructure/Operations Cybersecurity and Compliance at Thornton Tomasetti. **Topic:** Practical Cyber Security Assessments for Automation Systems. **Synopsis:** A typical vulnerability assessment has clearly defined objectives and technical procedures. But what happens when the assessor encounters an unfamiliar Industrial Control System (ICS)? Automation systems are popular in all industries, so how are they assessed for vulnerabilities? **Contact:** Ms. Plemons can be reached at Plemons.Erin@ensco.com. Ms. Hayes can be reached at LHayes@ThorntonTomasetti.com.

Do you want the ISSA-COS Online Program to continue on a weekly, biweekly, or monthly or 'not at all' basis if in-person presentations continue to be postponed due to COVID-19? If so, please email your preferences to execvp@ISSA-COS.org

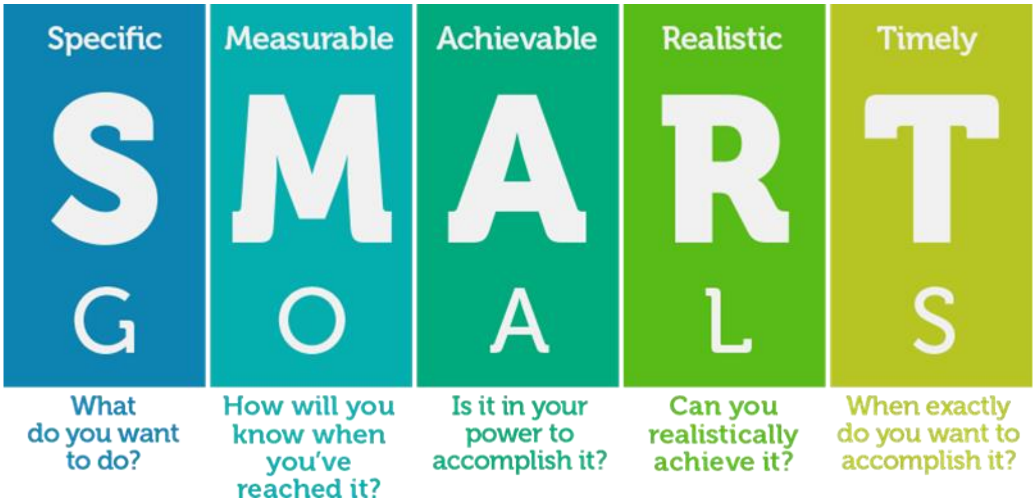
Mentoring Program

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:

- 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.

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


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

2020 Chapter Sponsors

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING
Platinum (ACS, CFS, PCS)

Jacobs
Bronze (ACS, CFS, PCS)

Hewlett Packard Enterprise
Bronze (CFS, PCS)

splunk>
EPOCH CONCEPTS
AGILE MINDS. POWERFUL CHANGE.
Bronze (CFS, PCS)

Venue Sponsors

L3HARRIS™ FAST. FORWARD.

NCC NATIONAL CYBERSECURITY CENTER

PIKES PEAK COMMUNITY COLLEGE

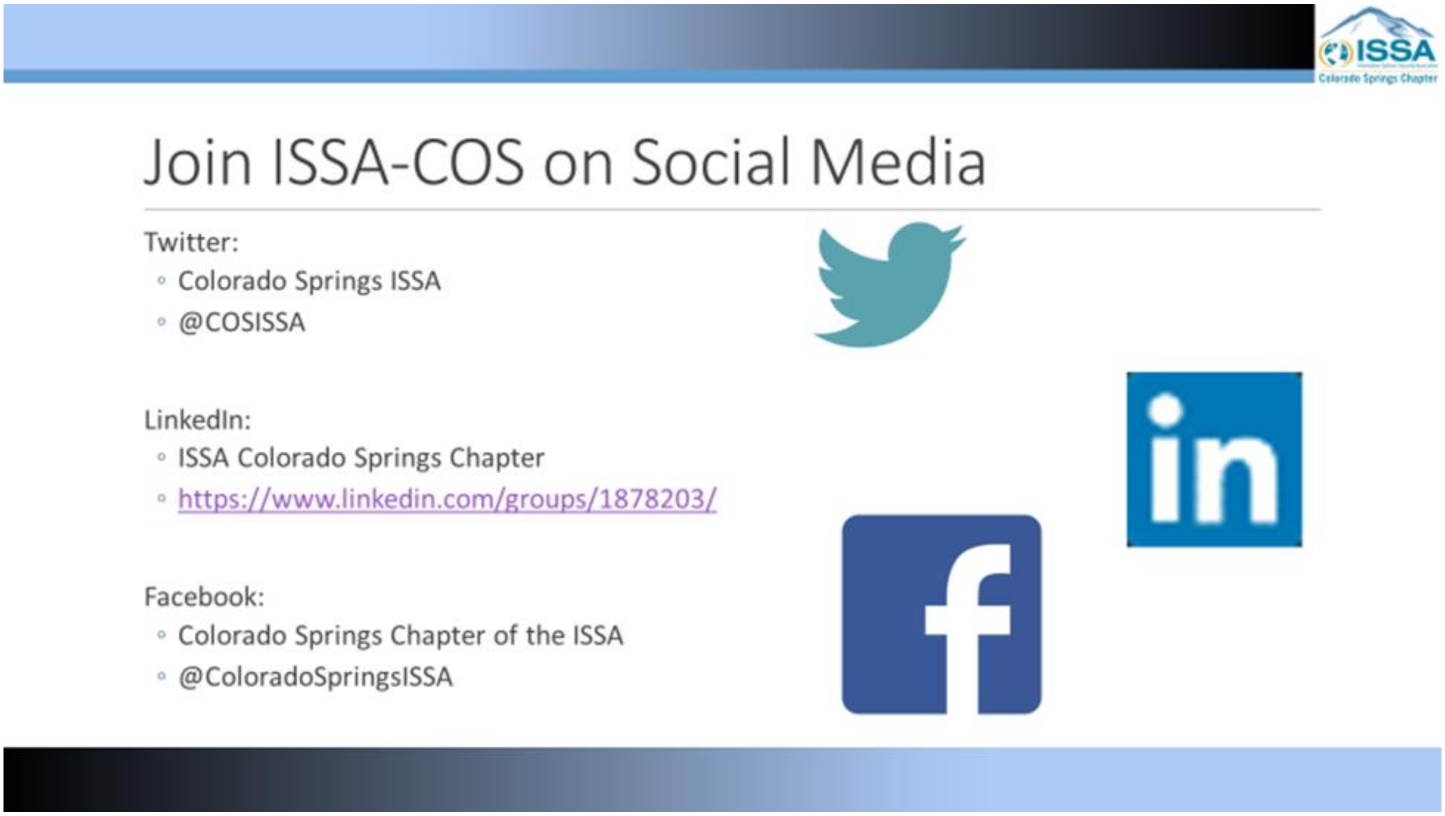
UCCS

Colorado Technical University

Become a Sponsor!

- **Annual Chapter Sponsor (ACS)**
- **Cyber Focus Symposium (CFS)**
- **Peak Cyber Symposium (PCS)**
- **Financial Sponsors**
- **Conference Exhibitors**
- **Material Sponsors**
- **Single Event Sponsors**

For more information about sponsorship opportunities, email: sponsorships@issa-cos.org



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

Strategic Partnership – NCX

Available Resources

- **ISSA-COS Agreement: CyberAlliance+**
- **Membership Plans**
- **Technical Forums**
- **LegalShield**
- **IDShield**
- **Pre-recorded Webinars**

ISSA-COS Community Partners

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
COLORADO SPRINGS WORLD AFFAIRS COUNCIL
U.S. AIR FORCE ACADEMY
NATIONAL CYBER EXCHANGE
OFFICIAL (ISC)² CHAPTER
AFCEA Rocky Mountain Chapter
CSBJ
COLLEGEAMERICA Since 1964
FIRMA IT
EMBRY-RIDDLE AERONAUTICAL UNIVERSITY
FOX21 NEWS
BLOCKFRAME
COLORADO PTAC GOVERNMENT CONTRACT ASSISTANCE
HANDSHAKE LEADERSHIP
Colorado Small Government Contractor Collaborative
UCCS
ManufacturersEDGE
Pikes Peak BUSINESS & EDUCATION ALLIANCE
PIKES PEAK WORKFORCE CENTER

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

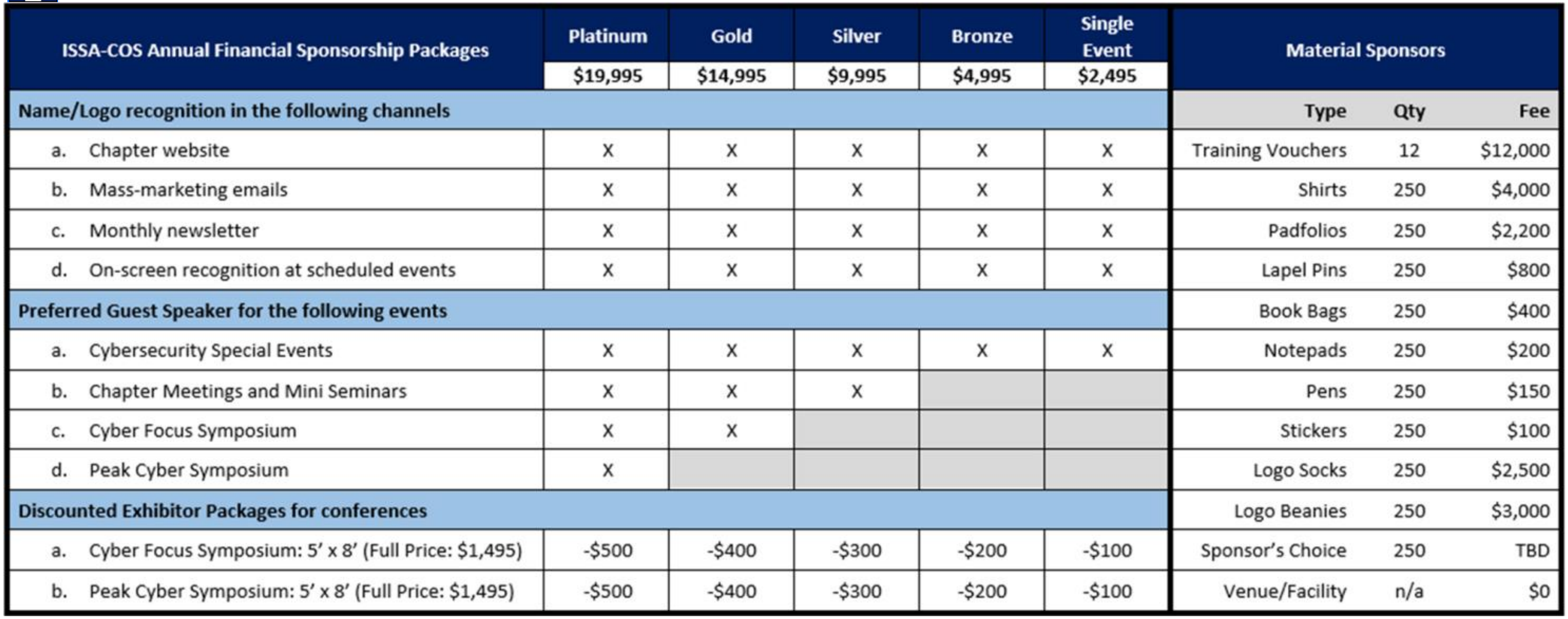
Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

Update Your Profile!

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

2020 Annual Chapter Sponsorship Plans

For more information email: sponsorships@issa-



ISSA-COS Annual Financial Sponsorship Packages	Platinum	Gold	Silver	Bronze	Single Event	Material Sponsors		
	$19,995	$14,995	$9,995	$4,995	$2,495			
Name/Logo recognition in the following channels						**Type**	**Qty**	**Fee**
a. Chapter website	X	X	X	X	X	Training Vouchers	12	$12,000
b. Mass-marketing emails	X	X	X	X	X	Shirts	250	$4,000
c. Monthly newsletter	X	X	X	X	X	Padfolios	250	$2,200
d. On-screen recognition at scheduled events	X	X	X	X	X	Lapel Pins	250	$800
Preferred Guest Speaker for the following events						Book Bags	250	$400
a. Cybersecurity Special Events	X	X	X	X	X	Notepads	250	$200
b. Chapter Meetings and Mini Seminars	X	X	X			Pens	250	$150
c. Cyber Focus Symposium	X	X				Stickers	250	$100
d. Peak Cyber Symposium	X					Logo Socks	250	$2,500
Discounted Exhibitor Packages for conferences						Logo Beanies	250	$3,000
a. Cyber Focus Symposium: 5' x 8' (Full Price: $1,495)	-$500	-$400	-$300	-$200	-$100	Sponsor's Choice	250	TBD
b. Peak Cyber Symposium: 5' x 8' (Full Price: $1,495)	-$500	-$400	-$300	-$200	-$100	Venue/Facility	n/a	$0

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**

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: 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***

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: Pat Laverty
Past President: Cindy Thornburg
Past President: Frank Gearhart
Past President: Colleen Murphy

Teenager Accused of Leading Ring of 'Evil Geniuses' on $24 Million 'Cybercrime Spree'

By Shoshana Wodinsky, Gizmodo, May 8, 2020

Yesterday, the prominent bitcoin investor Michael Terpin announced that he'd filed suit against the ringleader of a "SIM swap gang" that he'd been chasing down since 2018, following the theft of roughly a collective $24 million in bitcoin from his digital wallets. And it turns out the culprit, in this case, wasn't a criminal mastermind, but a shitty teenager.

That's according to the complaint Terpin filed yesterday against now 18-year-old Ellis Pinsky, a high school student in suburban New York who's currently "on track" to graduate high school. As Terpin explains, the then 15-year-old Pinsky led a 20-person "cybercrime spree" back in 2018 along with 20 other co-conspirators, netting themselves a collective $100 million in digital crypto in the process.

Read the rest here:

https://gizmodo.com/teenager-accused-of-leading-ring-of-evil-geniuses-on-2-1843348642

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