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

ISSA-COS NEWSLETTER
VOLUME 9 NUMBER 7 JULY 2020

Colorado Springs, Colorado

Welcome to July!

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.

Welcome to July! I hope everyone is doing well and staying healthy. I also hope folks have begun to spend time outside (safely of course) to enjoy the wonderful weather we have had lately. After the challenging months we have had, it feels good to step outside and just feel the warmth of the sun, breath the fresh air, and enjoy our beautiful scenery.

Looking back at the month of June, 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/sponsors: Checkmarx, Mr. Jeff Tomkiewicz, and the Info-Tech Research Group. Altogether, these knowledgeable and gifted speakers and sponsors provided our chapter and our community with valuable information and technology updates regarding various aspects of our industry and our professional development.

Also in full swing is the planning and preparation for the Peak Cyber Symposium (www.peakcyberco.com). Early bird registration remains open and offers FREE registration for all members of ISSA (regardless of their chapter affiliation), along with .mil, .gov, and .edu members of our community. Early bird registration is also being used to help gauge community interest and support for an in-person conference. If state restricts do not allow or if community confidence is low, we will need to consider shifting to a virtual or hybrid format. Please help support this event by sharing the promotional announcements via email and social media to all your professional contacts. The Call for Speakers is quickly closing however, the Call for Sponsors and Exhibitors remains wide open.

Looking forward to July, we will continue our online series with two new and exciting

(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.

Masked arsonist might’ve gotten away with it if she hadn’t left Etsy review

By Jon Brodkin, ArsTechnica, June 18 13, 2020

To some extent, every Internet user leaves a digital trail. So when a masked arsonist was seen on video setting fire to a police car on the day of a recent protest in Philadelphia, the fact that her face was hidden didn't prevent a Federal Bureau of Investigation agent from tracking down the suspect. The keys ended up being a tattoo and an Etsy review the alleged arsonist had left for a T-shirt she was wearing at the scene of the crime, according to the FBI.

The alleged arsonist—identified by the FBI as Lore-Elisabeth Blumenthal, 33—was wearing a mask, goggles, fire-resistant gloves, and a T-shirt with the slogan "Keep the immigrants, deport the racists" when her crime was captured live on an aerial news feed from a helicopter, FBI Special Agent Joseph Carpenter wrote in an affidavit filed Monday in US District Court for the Eastern District of Pennsylvania. After an investigation, she was arrested and charged with arson of two police vehicles. She appeared in federal court on Tuesday, and the government said it "will be filing a motion for the defendant to be detained pending trial."

> *“If convicted, the defendant faces a maximum possible sentence of eighty years in prison, followed by three years of supervised release, and a fine of up to $500,000.”*

In the news video, a police sedan was already "engulfed in flames" when the suspect "entered from the top of the frame and removed a flaming piece of a wooden police barricade from the rear window of the sedan that was already on fire, and then shoved the flaming wood into the SUV that was not on fire. Within minutes of that, the SUV was then completely engulfed in flames." This happened on May 30 after a protest over the death of George Floyd. The affidavit says, "While the protest earlier in the day was peaceful, violence erupted later on in the day," including the arson of police cars.

More footage of the arson came in a video posted on Vimeo that "clearly depicts the same female subject removing a flaming piece of wooden barricade from the marked PPD [Philadelphia Police Dept.] sedan and shoving it through the window of the marked PPD SUV," the affidavit said. An Instagram user had also posted a photo that "shows the female subject moving away from the sedan after it is on fire, and shows her backpack." The owner of the Instagram account provided more photos he had taken to the FBI, and another amateur photographer provided about 500 pictures taken that day in Philadelphia.

Even with video and photos, the FBI wasn't yet able to identify the suspect because her face wasn't visible. But the T-shirt she wore was unique and sold on Etsy, so FBI agents read the reviews on the seller's Etsy page to see if anyone from the Philadelphia area had purchased it. Blumenthal had left a 5-star review that said, "Fast shipping, thanks very much!" from her username "alleycatlore," and her Etsy profile displayed her location as Philadelphia, the affidavit said. The FBI did not yet have her full name, so they did a search for "alleycatlore" and found a user on the online fashion marketplace Poshmark "with a display name of 'lore-elisabeth,'" the affidavit said. A search for "Lore Elisabeth" in Philadelphia turned up "a LinkedIn profile for an individual matching the name 'Lore Elisabeth' who appears to be employed as a massage therapist with a company that provides massage therapy services."

Pictures of the alleged arsonist showed a tattoo of a peace sign on her right forearm, and that tattoo was visible in a four-year-old video of Lore Elisabeth performing a massage on her business's website. The website had a phone number for Lore Elisabeth, and Carpenter said the FBI used the Department of Homeland Security's Electronic System for Travel Authorization to confirm that the number "is associated with Lore Blumenthal," with an address on West Duval Street in Philadelphia. A further search of Pennsylvania Department of Motor Vehicles records found a DMV photo of Blumenthal along with her address and date of birth.

Read the rest here:

https://arstechnica.com/tech-policy/2020/06/masked-arsonist-mightve-gotten-away-with-it-if-she-hadnt-left-etsy-review/

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 June
Cecil Wilkinson
Curtis Brown
Matthew Smith
Halie Anthony
Vincent Persichetti
Curtis Brown
Matthew Smith
Halie Anthony
Vincent Persichetti

Good News! For those who have memberships about to expire or have expired, you can renew your membership with a $50.00 off discount. Simply go to https://www.members.issa.org/page/Renew and enter DISCOUNT CODE: 2020ISSA50. This offer expires 31 July 2020 so act fast! If you have issues with the discount code, contact memberservices@issa.org for assistance.

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 ~367 members as of the end of June 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

Update Your Profile!

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

(Continued from page 1)

A Note From Our President

presentations. On July 9th, ISSA-COS Past President Mr. Frank Gearhart will provide a presentation entitled: Quantum Cryptology and How it Impacts our Profession. Later in the month, on July 23rd, we look forward to spending the evening with a special guest speaker. Watch for further announcements coming soon! Please register early for these events and be sure to invite others as these events are open to the entire community.

Have you heard?! Members (to include recently expired members) can save $50 when renewing their membership before the end of July! Look for more information in this newsletter to include the super special promo code.

In closing, I remain proud of the many volunteers helping to keep our chapter up and operating. Special shout-outs to all our committees: IT Committee, Speakers Bureau Committee, Mentors Committee, and the Newsletter Committee. Together, their efforts help make our chapter one of the strongest chapters across the globe. Together, our chapter and our community work together for the betterment of everyone in it.

Sincerely,

Ernest

As cyber-criminals get more cunning, enterprise security must get smarter, with AI-augmented software as a weapon of choice

By Kurt Marko, Diginomica, June 24, 2020

Computer security has been a cat-and-mouse game between IT professionals and wily hackers since Robert Morris created the first network worm in the late 1980s. Ever since, hackers motivated by curiosity, animosity and, lately, greed have escalated their craft by devising more deviously sophisticated and stealthy techniques to enter (and sometimes corrupt) systems, exfiltrate data, compromise user credentials and steal personally identifiable information (PII). In response, IT organizations have deployed more elaborate security software with layered defenses, aggressive monitoring and more onerous authentication schemes. Every time IT applies new technology designed to block the latest attacks, hackers shift tactics.

No matter how much money and effort IT spends bolstering enterprise security, cyber-attackers remain undeterred and seemingly more successful than ever by focusing on the Achilles heel of IT security: users. Although conventional security measures have proven ineffective at blocking naive or careless user behavior, there is a reasonable prospect that a new generation of AI-enhanced security systems will succeed where less adaptive techniques have failed. Indeed, the time is ripe for data-driven machine and deep learning software to protect users from the most popular and effective attacks, phishing emails and messages.

Email is the preferred portal for data and identity theft

Massive thefts of corporate, government and personal data and identities, along with destructive ransomware and denial-of-service (DoS) attacks are so commonplace that they rarely make headlines, however, look deeper and the scope of the problem becomes evident. The FBI Internet Crime Complaint Center (IC3) is a clearinghouse for information about online criminal activity. The organization assists law enforcement and industry cybersecurity groups by investigating and analyzing reported cases of fraud, IP theft, system intrusions, extortion and identity theft.

The most recent 2019 IC3 annual report shows that cyber-crime is a thriving activity.

- Complaints have gone up 1.6-times in four years, a CAGR of 13%.
- Financial losses have increased 3.2-times for a 34% CAGR since 2015.

So called Business Email Compromise (BEC) / Email Account Compromise (EAC) account for about half the overall monetary damage with losses of over $1.7 billion in 2019. In an interview with cyber-security researcher Brian Krebs, a security engineer at Flashpoint said the percentage was even higher at 63 percent of fraud losses reported to the FBI.

Read the rest here:

https://diginomica.com/cyber-criminals-get-more-cunning-enterprise-security-must-get-smarter-ai-augmented-software-weapon

Remote Working: Are You Really Secure?

By Andrew Milne, CISO Mag, June 23, 2020

As cities across the globe begin to ease their COVID-19 restrictions, this year's transition back to the office could take place in stages — or not at all. Prior to the pandemic, data had already shown a steady increase of remote work employees — growing by 173% over the last 15 years, with nearly 5 million telecommuters in the U.S. alone.

Research now shows nearly 40% of global companies expect work-from-home policies to be permanent. Supporting this data, a study last month shows 65% of UK workers believe remote working could become more common after COVID-19. In Canada, 66% of Canadians who shifted to remote work earlier this year, reported a high success rate.

While businesses and organizations consider their next steps, what impact will this have on your cybersecurity strategies?

Working Safely, Securely, and Remotely

Whether you are transitioning back to the office or working remotely long-term, cybersecurity best practices remain as important as ever — and it is equally critical that employees stay vigilant about new COVID-19 scams, and web and email threats.

You can also bet that cybercriminals are tracking these next steps. One look at this year's cybercrime numbers, provides a good reminder.

Consider these recent risks, in just the first quarter of the year:

Over 25,000 malicious COVID-19 websites were created on March 19 — a record for the first quarter.

In March, phishing and counterfeit websites increased to 8,342 — from just 3,142 in January.

More than 80% of remote work employees surveyed recently claimed awareness of COVID-19 phishing scams, yet 24% clicked on a link from an unknown sender before determining their legitimacy and only 12% reported the email.

An estimated 36% of these employees are using one or more personal devices to access company files and 29% also share that device with other members of their household.

The reality is, as lockdown restrictions change, you should not change the attention placed on cybersecurity and remote work risks.

Secure your teams working from any location

As companies consider their transition options, ensuring employees can work from any location, productively and securely — without compromising the security of networks, devices, and users — remains a critical challenge.

That is why our team at Field Effect recently introduced Covalence for Remote Work.

Based on the technologies and capabilities of our flagship Covalence threat detection and monitoring platform, Covalence for Remote Work provides a complete solution in one platform for monitoring and detecting cyberthreats to email and cloud services, devices that support remote work, vulnerabilities in cloud networks, and more.

Here is a quick look:

- **Personalized cloud security monitoring:** Gain the insights to detect malicious or suspicious activity to your endpoint devices, email, and cloud services. Covalence uses data, logs, and APIs from your cloud service providers to monitor and identify threats to your services, administrative components, user accounts, and more.
- **Advanced monitoring and analytics:** Benefit from machine learning and cloud analytic capabilities that provide continuous analysis of user and service data to identify threats. The result is real-time visibility to detect, monitor, measure, manage, and reduce attackable points.

Simple, affordable, powerful: Priced affordably, Covalence integrates easily with all existing systems. Set it up in just a few clicks and it does the heavy lifting to protect you as quickly as possible.

Read the rest here:

https://cisomag.eccouncil.org/remote-working-are-you-secure/

Hackers Using Steganography to Target Industrial Enterprises: Kaspersky

By Staff, CISO Mag, June 2, 2020.

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.

Security experts from Kaspersky have warned about a series of attacks targeted at distributors of equipment and software for industrial enterprises globally to steal Windows credentials. It is found that attackers are using phishing scams and steganography methods to hide malware on legitimate image and file resources.

In its report, Kaspersky stated that it identified a series of targeted attacks on organizations located in Japan, Italy, Germany, and the U.K. from May 2020. Hackers used malicious Microsoft Office documents, PowerShell scripts, and other sophisticated techniques like steganography to escape detection. While the ultimate goal of the attackers is unknown, Kaspersky stated that hackers used Mimikatz utility to steal the authentication data of Windows accounts stored on a compromised system.

“Phishing emails, used as the initial attack vector, were tailored and customized under the specific language for each specific victim. The malware used in this attack performed destructive activity only if the operating system had a localization that matched the language used in the phishing email,” researchers said.

Steganography

Steganography is an ancient practice of hiding secret content and text messages inside non-suspicious messages. Cybercriminals use this technique to hide malicious code within the image/audio/text file that is mainly employed by exploiting kits to hide their malvertising traffic. If the victim clicks the document, the script will execute and downloads the image hosted online which contains the malicious code.

Attack Chain

The phishing emails from attackers contain an urgent request to open the malicious attachment. Hackers send an Excel spreadsheet with a malicious macro or a malicious image (using Steganography technique) and ask users to enable active content, which triggers the malicious PowerShell script. The hidden malware will be executed when the user downloads the malicious excel sheet or the image.

“The data is hidden in the image using steganographic techniques and is extracted by the malware from pixels defined by the algorithm. Using steganography enables the attackers to evade some security tools, including network traffic scanners. The data extracted from the image is consecutively encoded using the Base64 algorithm, encrypted with the RSA algorithm and encoded using Base64 again,” researchers added.

Preventive Measures

Kaspersky has also listed certain preventive measures to mitigate these kinds of attacks, these include:

- Train employees at enterprises in using email securely and, specifically, in identifying phishing messages
- Restrict macros in Microsoft Office documents
- Restrict PowerShell script execution
- Pay special attention to events of launching PowerShell processes initiated by Microsoft Office applications
- Restrict the ability of programs to gain SeDebugPrivilege privileges

Read the rest here:

https://cisomag.eccouncil.org/hackers-using-steganography-to-target-industrial-enterprises-kaspersky/

'Offensive capability': $1.3b for new cyber spies to go after hackers

By Anthony Galloway, The Sydney Morning Herald, June29, 2020

Australia will recruit 500 cyber spies and build on its offensive capabilities to take the online fight overseas in a $1.3 billion funding boost, amid rising tensions with China and a growing wave of attacks against the nation's critical infrastructure.

The Australian Signals Directorate will also share intelligence with government departments and companies in near real time as part of the biggest ever cash injection to Australia's cyber defences.

Prime Minister Scott Morrison will on Tuesday announce the ASD will be given more than $1 billion over the next decade to disrupt foreign cyber criminals and better identify malicious hacks.

The funding announcement comes amid an escalating wave of cyber attacks against Australian governments and businesses, including critical infrastructure such as hospitals and state-owned utilities.

Australian security agencies believe China is behind the cyber raids on all levels of government, although the Morrison government has chosen not to name the country involved.

Under the plan, Australia's chief cyber defence agency will be given $31 million to build new offensive capabilities to go after cyber attackers offshore and disrupt their activities before they have the chance to strike at Australian governments and businesses.

There will also be a new $25 million cyber threat-sharing platform, allowing industry and government to share intelligence about malicious cyber activity and block emerging threats in near real-time.

The ASD will be given new capabilities to allow the agency and Australia's major telcos to prevent malicious cyber attacks ever reaching millions of Australians by blocking known malicious websites and computer viruses more quickly.

The cyber body - which is part of the Department of Defence - will also be given $118 million to expand its data science and intelligence capabilities to identify emerging cyber threats to Australia over the next 10 years.

Prime Minister Scott Morrison said malicious cyber attacks against Australia were increasing in frequency, scale and sophistication.

"The federal government's top priority is protecting our nation's economy, national security and sovereignty. Malicious cyber activity undermines that," Mr Morrison said.

"My government's record investment in our nation's cyber security will help ensure we have the tools and capabilities we need to fight back and keep Australians safe."

The added capabilities for the ASD will form part of Australia's new four-year cyber security strategy, which will be released in the next few months.

There is still more than $500 million out of the $1.35 billion funding injection yet to be announced, which is expected to be detailed in the new strategy.

The NSW government was a major target of the cyber attacks carried out in recent months, which alarmed Australian security agencies and sparked Mr Morrison to publicly warn Australians about the rise in attacks against the nation's critical infrastructure - but he stopped short of naming Beijing.

China has denied it was behind the wave of cyber attacks in Australia, saying the claims were "baseless".

The Morrison government has previously warned power stations, transport systems and industrial plants are likely to be the target of cyber attacks from state-sponsored hackers and criminal networks.

The government has recruited former US secretary of homeland security Kirstjen Nielsen to help prepare the cyber security strategy.

Read the rest here:

https://www.smh.com.au/politics/federal/offensive-capability-1-3b-for-new-cyber-spies-to-go-after-hackers-20200629-p557bk.html

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/_QtQ0l9nkskTqK4YDlJgaD08HQQ=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

Demystify Regulatory Compliance in the Cloud

By Aj Yawn, CISO Mag, June 26, 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.

In the recent CISO Mag Cloud Security Survey – June 2020, one of the questions posed to respondents was "What are some of the biggest security concerns raised when you choose a cloud service provider (CSP)?" A notable finding was that more than two-thirds of respondents stated that regulatory compliance is a key security concern when choosing a cloud service provider. The major cloud service providers — Amazon, Google, and Microsoft — address regulatory compliance head-on and painstakingly educate their customers on the shared responsibility model. This article will aim to help security leaders solve the dynamic and evolving problem with regulatory compliance on the cloud.

An understanding of the shared responsibility model and its relationship to regulatory compliance will assist security leaders in preparing for regulatory compliance assessments when hosted on the cloud. Cloud security is a shared responsibility, this shared responsibility extends to regulatory compliance. The cloud shared responsibility model outlines that CSPs are responsible for the *security **of** the cloud* and customers are responsible for *security **in** the cloud* (securing the data they put in the cloud). Customer or CSP responsibility shifts depending on the cloud computing deployment type – IaaS, PaaS, or SaaS.

Regulatory compliance should be viewed through this same security shared responsibility model. The CSPs are responsible for maintaining and proving the regulatory compliance **of** the cloud, while customers are required to maintain and prove regulatory compliance of the data and applications they host **in** the cloud. The CSPs do a great job of demonstrating compliance and making this information available to its customers.

AWS, Microsoft, Google, and the other CSPs make information regarding their achieved compliance certifications readily available to all their customers. A quick glance at the three major CSPs security and compliance web pages, and you can see that they all maintain several recognized industry certifications such as SOC 2, ISO 27001, and HIPAA.

My CSP is compliant, how does this impact my organization?

These compliance certifications enable an organization to leverage the cloud service providers but they do not replace the cloud consumers' requirement to perform their own third-party assessments. In certain instances, compliance frameworks allow organizations to leverage the controls in place at their CSPs for their compliance assessments. For example, in a SOC 2 assessment, you will see CSPs referred to as "subservice organizations." This means that the CSP is implementing certain controls on behalf of their customers; these controls include physical and environmental security controls for the facilities where the data resides.

These physical and environmental security controls are only a subset of a complete cybersecurity audit. This is where customer responsibility begins with regulatory compliance in the cloud. The customer, your organization, is responsible to prove how they are addressing other common domains such as access control, risk management, onboarding procedures, termination, network security, change management, and vendor management. This is generally accomplished through evidence collection procedures, interview discussions, and observations with third-party auditors.

Ok, I understand shared responsibility, but what about data sovereignty? Is that shared too?

A regulatory compliance concern that is fairly common amongst security professionals as they are migrating to the cloud is regarding data sovereignty laws. In fact, 59% of survey respondents noted data ownership as a key security concern when choosing a cloud service provider and 47% of respondents cited data location as a security concern.

Data sovereignty is the idea that your data is subject to the laws and governance structures within the nation where it is collected. The concept of data sovereignty is closely linked with data security, cloud computing, and technological sovereignty. Understanding the shared responsibility model addresses data sovereignty concerns because you understand your responsibility and control with respect to the data hosted in the cloud. As a reminder, you, the customer, are responsible for security ***in*** the cloud. Specifically, you are completely responsible for your data. Pursuant to this responsibility, organizations have complete control over where their data is stored and how it is managed (backup, retention, encryption, etc.).

Read the rest here:

https://cisomag.eccouncil.org/regulatory-compliance-in-the-cloud/

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)

This training tool could be the answer to stop mass cyberattacks

By Mark Pomerlieau, C4ISRNet, June 25, 2020

At air bases across Europe, networks are under attack. Malicious hackers have gained access to sensitive systems, information, controls and critical infrastructure. But cyber operators from U.S. Cyber Command, in concert with Five Eyes partners, have been called in to thwart these attempts in real time.

This was the main scenario for this year's capstone cyber training exercise put on by Cyber Command, Cyber Flag 20-2.

The exercise, which took place June 15-26 and was exclusively defensive in nature, saw more than 500 participants and 17 teams participating from five countries across nine time zones, and it included America's National Guard, the U.S. Energy Department and the Five Eyes alliance — Australia, Britain, Canada, New Zealand and the U.S. Australia, however, did not participate during this iteration.

Officials told reporters this week that the purpose of Cyber Flag 20-2 was to continue building the community of defensive cyber operations and to improve the overall capability of the Five Eyes countries to defend against cyber aggressors.

The drill involved teams defending IT and operational security networks against a live, opposing force trying to disrupt, deny and degrade the air bases' operations. The networks under attack were industrial control systems simulated to generate network traffic for an aviation fuel farm, power grid, air traffic control radars and electronic access control systems. The attacks came in the form of malware that targeted devices responsible for fuel and power.

But the unique aspect of this year's exercise, as C4ISRNET previously reported, was the use of a new remote cyber training tool called the Persistent Cyber Training Environment.

PCTE is an online client that allows Cyber Command's cyber warriors, as well as partner nations, to log on from anywhere in the world to conduct individual or collective cyber training as well as mission rehearsal, which to date had not existed for the cyber force as it does for physical troops.

The program is run by the Army on behalf of the joint cyber force. The platform not only allowed the exercise to continue as planned amid the coronavirus pandemic, but it enabled collaboration and simultaneous training across the world.

A new way to train

Officials say PCTE is providing Cyber Command with an entirely new way to train cyber forces, which previously was difficult given a lack of infrastructure and the time needed to set up ranges and scenarios.

It also allows Cyber Command and military units to conduct more frequent training. Cyber Flag typically was Cyber Command's largest and only holistic tactical training event, held annually during June. For units, aside from Cyber Flag, there were no other ways to stay sharp on their skills unless they built their own environments.

Read the rest here:

https://www.c4isrnet.com/dod/cybercom/2020/06/25/this-training-tool-could-be-the-answer-to-stop-mass-cyberattacks/

Why pay attention to indictments of foreign hackers?

By Derek B. Johnson, FCW, June 19, 2020

For the past three and a half years, the U.S. government has carried out a deliberate strategy to "name and shame" state-aligned hacking groups for norm-busting behavior in cyberspace, usually in the form of highly detailed indictments.

The Department of Justice uses these to reveal how these groups operate, who they are and what sector or organizations they're targeting. Often they include highly personal details about the individuals involved, including photos, biographical information and place of employment for individual hackers.

Some detractors wonder if these indictments are just public relations campaigns, since those identified typically are outside the reach of U.S. and international law enforcement. Others have warned the efforts will lead to similar retaliation against U.S. cyber operatives.

Assistant Attorney General for National Security John Demers said the department is also banking on other second and third order effects when they out foreign operatives and their work.

Speaking at the Defense One Tech Summit June 18, Demers noted that indictments can be effective if charged individuals travel to countries that have extradition treaties in place with the U.S. government. Such instances are rare but do happen, as it did with Yanjun Xu, a Chinese Ministry of State Security officer who was arrested in Belgium and extradited to the U.S. on charges of stealing trade secrets from U.S. aviation firms.

But bringing charges against these groups gives the department a way to broadly communicate with a different audience: domestic victims of these campaigns inside the U.S., many of whom may be unaware just how intensely they're being targeted.

He used the 2018 indictments of the Mabna Institute and nine associated individuals as an example. The document outlined how the Iranian-linked organization targeted hundreds of universities and thousands of individual professors to steal sensitive technology and research. Follow up research by put out a week later by PhishLabs also illustrated how the organization conducted "general targeting of university students and faculty" in order to collect library account credentials.

"You can take that indictment and go to the research institutions, and you're not just saying 'I'm warning you these things are happening'…that is an indictment that tells a story that is understandable and is all unclassified, so it has an educational aspect as well.

It can also focus legislative efforts: this month a group of senators led by Rob Portman (R-Ohio) and Tom Carper (D-Del.) cited intellectual property theft by Iran and other nations while introducing a bill that would require organizations who sponsor foreign exchange students to put in place additional safeguards if those students will have access to sensitive technologies.

Another audience DOJ is hoping to reach: hackers in Russia, China or Iran who moonlight for their governments but also have "other business interests" that wouldn't benefit from the increased international scrutiny that comes with being named in U.S. charging documents. While a military officer with a nation state "is very rarely deterred by the possibility of indictment," those contractors, particularly ones in the early stages of their careers, might have a different risk calculus.

Read the rest here:

https://fcw.com/articles/2020/06/19/johnson-doj-hacker-indictments.aspx?admgarea=TC_Security1

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.

Peak Cyber Symposium – *10th Anniversary!*

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

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.

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.

Peak Cyber Symposium

KEYNOTE SPEAKERS

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

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

JUST CONFIRMED!

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

JUST CONFIRMED!

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

Nathan Toups
Senior Site Reliability Engineer
Santé Capital
Quantitative Hedge Fund

JUST CONFIRMED!

Karen Worstell
CEO
W Risk Group

Early Bird Registration is now open.

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

www.peakcyberco.com

Frank Gearhart

ISSA-COS Online Series July 2020 – Session 1

Date: July 9, 2020, 6 – 7:30 PM

Guest Speaker: Frank Gearhart, C|CISO, CISSP, C|HFI, C|NDA

Title: Quantum Cryptology and How it Impacts our Profession

Synopsis: Practical quantum computing—assuming it is achieved—will have tremendous impacts on our global information society and could help solve currently intractable problems. Quantum cryptology could break the encryption algorithms that protect our financial, commercial, industrial, defense, and individual data systems. But quantum cryptology depends on capable and stable quantum computing, which currently face significant challenges. We'll look at some of the current research in quantum cryptology, some recommendations, and what we might expect from quantum cryptology in the near future.

Register at: www.issa-cos.org

07/09/2020 / Session 1

- **Speakers: Mr. Frank Gearhart,** *C|CISO, CISSP, C|HFI, C|ND, ISSA-COS Past President*
- **Topic: Quantum Cryptology and How it Impacts our Profession**

07/23/2020 / Session 2

- **Speaker: Reserved**
- **Topic: TBA…wesome!**

08/06/2020 / Session 1

- **Speaker: This could be YOU!**
- **Topic: TBD**

08/20/2020 / Session 2

- **Speaker: This could be YOU!**
- **Topic: TBD**

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

Register at: www.issa-cos.org

JUNE 2020 LEGAL REPORT

By Sara Mosqueda, Security Management, June 1, 2020

Judicial Decisions

Hacking. A U.S. federal court ruled that academic researchers testing online hiring platforms for discrimination did not violate a federal hacking law.

Researchers Christian Sandvig, Kyratso Karahalios, Christopher Wilson, and Alan Mislove—working with nonprofit journalism group First Look Media Works, Inc.—said they planned to create fake job listings and profiles for fake job applicants to discover whether online job listing websites' algorithms skewed candidates' rankings due to race, gender, age, or other characteristics protected by U.S. civil rights laws. At the time of the court's ruling, the researchers had not identified which websites they will test.

Concerned that the federal government would criminalize their future research, the researchers filed a preemptive suit against U.S. Attorney General William Barr, claiming that provisions of the Computer Fraud and Abuse Act (CFAA) violated the First and Fifth Amendments of the U.S. Constitution—the freedom of speech and the right to due process clauses, respectively. The CFAA criminalizes intentionally accessing a protected computer or website like LinkedIn without authorization.

Judge John Bates dismissed the case, bypassing the constitutional argument and determining that even if the research would violate a website's terms of service—which could lead to civil liabilities—it would not constitute criminal liability under the CFAA. Most password-protected servers or websites have terms of service that allow permission in exchange for accurate information about a user. If such violations were criminalized, it would risk allowing terms of service for all websites to become individual laws, enacted by companies instead of governments. "Such an arrangement …would raise serious problems," Judge Bates wrote.

Also, the researchers said they had no intention of bypassing any of the websites' permission requirements, "and thus none of them when executed will constitute violations of the CFAA as interpreted," Bates added. (*Sandvig v. Barr,* U.S. District Court of the District of Columbia, No. 16-1368-JDB, 2020)

Age discrimination. The Jet Propulsion Lab (JPL) for the National Aeronautics and Space Administration (NASA) agreed to pay roughly $10 million to settle claims of age discrimination brought by the U.S. Equal Employment Opportunity Commission (EEOC).

The EEOC said that since 2010, the spacecraft laboratory had "systematically, disproportionately adversely impacted employees aged 40 and older for layoff and rehire compared with employees aged 39 and younger," according to the complaint filed in court.

The lab settled the claims before reaching a jury trial and also agreed to appoint an employment monitor, a diversity director, and a layoff coordinator. On top of this, for the next three years JPL will report certain data on dismissed employees and employee complaints to the EEOC. (*U.S. Equal Employment Opportunity Commission v. Jet Propulsion Laboratory et al.,* U.S. District Court for the Central District of California, No. 2:20-cv-03131, 2020)

Kidnapping. A Pakistani court overturned the death sentence of British-born Ahmed Omar Saeed Sheikh, who was convicted of the 2002 kidnapping and murder of *Wall Street Journal* journalist Daniel Pearl.

While Sheikh was involved in Pearl's kidnapping, his direct involvement in Pearl's death remained disputed. After years of appeals, the high court of Sindh upheld only the kidnapping charge and its seven-year prison sentence. As of *Security Management's* print deadline, Sheikh was awaiting release orders after serving 18 years in prison.

Sheikh's three other Islamist militant co-defendants were serving life sentences for their involvement. The court also acquitted them of the charges.

Pakistani prosecutors said in a statement that they will probably file an appeal with the country's supreme court.

The Pearl Project, an independent investigative project out of Georgetown University, maintained that the original trial against Sheikh and the three other men used perjured testimony to secure a speedy conviction. The project claimed that while the four men were involved in the kidnapping, a total of 27 men were allegedly involved in Pearl's murder. (*Ahmed Omar Sheikh v. The State,* High Court of Sindh, Principal Seat Karachi, No. 87-73025, 2020)

Legislation

Read the rest here:

https://www.asisonline.org/security-management-magazine/articles/2020/06/june-2020-legal-report/

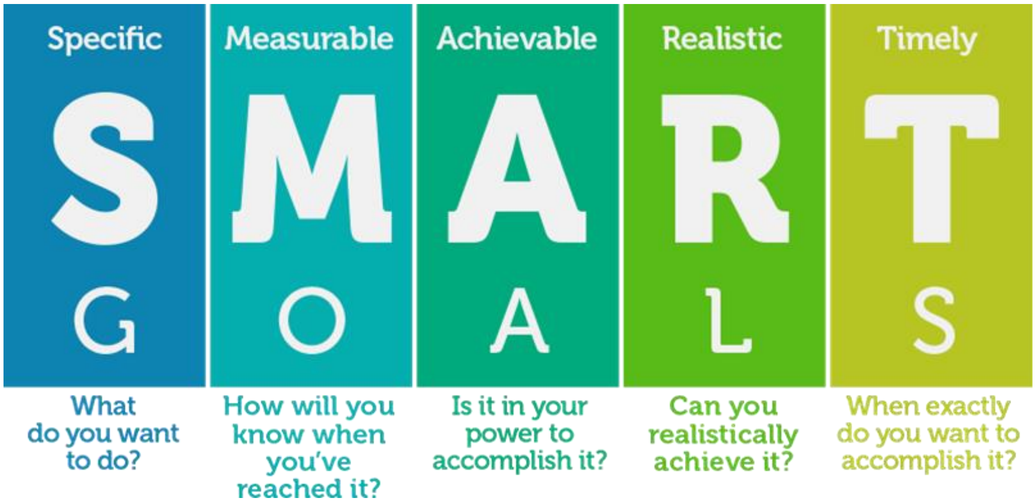
MENTORING PROGRAM

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?

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**

Passwords are a government security nightmare

By John Hertrich, GCN, June 12, 2020

The Small Business Administration blamed an internal error for its recent leak of at least 8,000 Economic Injury Disaster Loan applications. Whether or not a “glitch” is to blame (many officials doubt that it is), this latest headline-making blunder reminds government agencies to review how they’re preventing sensitive data from ending up in the wrong hands.

Such news stories attract hackers to government agencies like moths to a flame; it tips them off to which agencies are likely still using antiquated techniques to protect their treasure trove of Social Security numbers, employee credentials, tax IDs and more. Hackers also know that agencies have been forced to quickly shift to remote work during this global pandemic and are scrambling to maintain security in a new, complex environment.

There’s a simple security measure that could take phishing attacks out of the equation and remove one of hackers most useful tools: getting rid of passwords.

Given the number of breaches due to password theft, it’s a wonder agencies are still using passwords despite their high risk exposure. According to research from Verizon, over 80% of all data breaches involve stolen passwords, making it time to stop pretending passwords are still an effective security measure.

Employee risk factors

Nearly 90% of successful data exfiltrations and breaches in the federal government over the past few years were the result of phishing attacks, according to the director of the National Counterintelligence and Security Center. This is an even bigger threat as government employees working remotely are downloading new tools daily and accessing various networks. In a work from home (WFH) environment, security and IT teams have very little control or oversight. While it’s tempting to believe everyone is following exemplary security practices, the reality is that government employees are reusing passwords just like everyone else.

This means that passwords used for sensitive government activities may also be used on consumer sites at risk of being hacked. Recent breaches at HomeChef and EasyJet put consumer login information at risk, but it’s the breaches that haven’t been publicized that place users at greater risk. With the average person reusing their favorite password at least 14 times, it’s easy to do the math and see the size of this risk.

Passwords are a liability

Of course, it’s users’ responsibility to keep the password to themselves. For a password to work, however, organizations must know the password to verify it. This is typically done in a secure database known as a credential vault. Just as criminals rob banks because that is where the money is, hackers break into credential vaults because that’s where all the passwords are. This makes the use of passwords a liability to the organizations that use them to secure critical data..

Hackers seek out passwords

Hackers can often take advantage of poor security settings and compromise the credential vault that stores all of a network’s usernames and passwords. More often than not, however, all hackers really have to do is send users an email tricking them to give up their password. In 2018, the Defense Information Systems Agency reported that the Defense Department had fended off 36 million malicious emails from hackers containing phishing schemes, malware and viruses. With one simple click of a link in an email, users are whisked away to a site that looks just like a page they are familiar with, and in seconds they can share critical login credentials.

If this seems too easy, there are a host of other far more sophisticated schemes in hacker’s tool chest, including keystroke loggers, spyware or mobile malware. If passwords were supposed to be a secret, then this is a good reason why they are not working.

There are other options

Read the rest here:

https://gcn.com/articles/2020/06/12/eliminate-passwords.aspx?admgarea=TC_SecCybersSec

Working from home on your own PC? Security is still a confusing mess for many

By Steven Ranger, ZDNet, June 23, 2020

Many companies have spent the last couple of months scrambling to deploy new systems to manage the security risks surrounding remote working. And with working from home likely to become much more prevalent, it seems there's still plenty more work to do.

For most staff, remote working has been a new experience: more than 80% of respondents said they either rarely worked from home or not at all prior to the pandemic, according to research by IBM.

But half of the 2,000 remote workers who responded said they were doing so with no new security policies to help guide them; a similar proportion said they were worried about security threats in their new home-office settings.

"Business activities that were once conducted in protected office environments, and monitored under specific policies, have quickly transitioned to new, and potentially less secure territory," said IBM, pointing to the example of customer service agents who worked in closely managed call centers, but who are now managing sensitive customer data at home.

Workers seem confident in their employers' ability to keep personally identifiable information secure while working remotely. But over half are also now using their personal laptops for work, and 61% said their employer has not provided tools to properly secure these devices.

More than half also said they have not been provided with new guidelines on how to handle highly regulated data while working from home. Two thirds said they have not been provided with new password management guidelines, while a third are still reusing passwords for business accounts.

Read the rest here:

https://www.zdnet.com/article/working-from-home-security-is-still-a-confusing-mess/

Air-Gapped Systems are Becoming a Treasure Trove for Attackers

By Staff, Cyware Social, June 14, 2020

For years, air-gapping has been recommend as a standard cybersecurity practice to protect sensitive systems and networks. Often, organizations isolate their critical systems by disconnecting them from the public internet or other networks to protect sensitive data and backups from cybercriminals. However, this technique is not proving to be a magic bullet as it once was.

Why the rising concern?

Last month, three reports showed an increased interest of hacking groups toward developing malware capable of infiltrating air-gapped networks. Let’s find out!

The Chinese hacking group, Tropic Trooper, also known as KeyBoy targeted the air-gapped networks of Taiwan and the Philippines military. According to Trend Micro, a cybersecurity and defense company, the attacks embraced the use of USBferry, a malware strain with a feature that allows self-replication to removable USB devices.

Researchers at ESET, the cybersecurity firm, discovered a malware called Ramsay that is capable of jumping the air gap to collect Word, ZIP files, and PDFs in a hidden storage container. Once the malware enters an air-gapped device, it can spread to any other device it may find.

Security researchers at Kaspersky identified a new version of the COMpfun malware used by Turla, a state-sponsored Russian threat actor. The new malware contains a self-propagation mechanism to infect other systems on internal or air-gapped networks.

After three back-to-back attacks on air-gapped networks within a week in May, Kaspersky revealed a new malware called USBCulprit in the first week of June. Used by a hacking group known as Cycldek, Goblin Panda, or Conimes, the malware is designed to compromise air-gapped devices via USB to steal government information.

Read the rest here:

https://cyware.com/news/air-gapped-systems-are-becoming-a-treasure-trove-for-attackers-f109e579

Colorado Springs Chapter

WWW.ISSA-COS.ORG

The Information Systems Security Association (ISSA) ® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Chapter Officers:

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

Recorder/Historian: Andrea Heinz
- Deputy: **Vacant**

Dir. of Professional Outreach: Katie Martin
- Deputy: **Vacant**

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: Steven Mulig
- Deputy: **Vacant**

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

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

Committee Chairs:

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

**** Executive Board Members***

Article for the Newsletter?

We are always looking for articles that may be of interest to the broader Colorado Springs cyber community.

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Past Senior Leadership

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

Light Bulbs Now Got Ears: New Eavesdropping Technique May Leak Your Conversations

By Staff, Cyware, June 18, 2020

In a new experiment, some researchers have successfully demonstrated that it is possible to track and recover any conversations by closely observing the light bulbs.

Academics from the Ben-Gurion University of the Negev have discovered a new way to reverse engineer and thus hack any conversations or audio recordings being played in a room, by observing the fluctuations of a light bulb in that room.

Read the rest here:

https://cyware.com/news/light-bulbs-now-got-ears-new-eavesdropping-technique-may-leak-your-conversations-aaacfd90

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