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

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 5 MAY 2019

Colorado Springs, Colorado

A Special Opportunity

ISSA-COS Members,

In addition to our normal monthly programming, the month of May will include a very special opportunity for our chapter. By way of our relationship with the COS Chamber and EDC, we received a request from the U.S. Department of State (DoS) to host a Mongolian delegation of National Cybersecurity Officials. This nine (9) person delegation is seeking tips and recommendations on how best to implement robust policies and procedures onto the foundational implementation of a nation-wide cybersecurity capability. ISSA-COS will serve as host, moderator, and panel planning committee for this event. What an honor for our organization!

Further down the road, the month of June will include our second gathering of Special Interest Groups (SIGs). In this gathering, we will launch a new SIG: **E *[ducators]* in Security (EduIS)**. This SIG will focus on providing educational tips and suggestions to instructors and educators in our community at both the K-12 and collegiate levels. Invite your instructors, your children's teachers, and anyone you know who participates in helping educate our future generation of Cybersecurity professionals.

Also scheduled for the month of June, is our annual CISSP Review. This year, our CISSP Review has been compressed to one month and will include two Friday evening sessions and four Saturday sessions. The reason for the compressed schedule is to decrease the commitment require by both participants and instructors. The compressed format will also increase memory retention by not stretching the learning curve across two or even three months. If you are interested in participating, please register now!

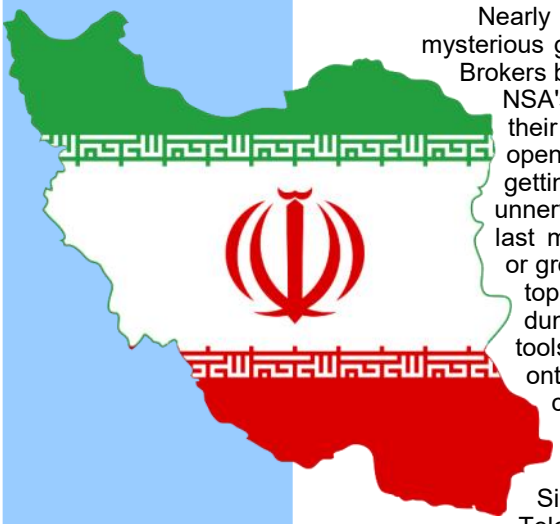
A Note From Our President

By Mr. Ernest Campos

Finally, it isn't too early to look ahead towards our annual Peak Cyber conference. This year, Peak Cyber will be held on September 3rd, 4th, and 5th. For this year's conference, ISSA-COS and the Federal Business Counsel (FBC) are looking to significantly increase participation among the Healthcare, Finance, Educational, and Retail industries. Yes, our

(Continued on page 5)

A Mystery Agent is Doxing Iran's Hackers and Dumping Their Code



By Andy Greenberg, Wired, April 18, 2019

Nearly three years after the mysterious group called the Shadow Brokers began disemboweling the NSA's hackers and leaking their hacking tools onto the open web, Iran's hackers are getting their own taste of that unnerving experience. For the last month, a mystery person or group has been targeting a top Iranian hacker team, dumping their secret data, tools, and even identities onto a public Telegram channel—and the leak shows no signs of stopping.

"We don't often get a look into state-sponsored groups and how they operate," he says. "This gives us some idea of the scope and scale of this group's capabilities."

Since March 25, a Telegram channel called Read My Lips or Lab Dookhtegan—which translates from Farsi as "sewn lips"—has been systematically spilling the secrets of a hacker group known as APT34 or OilRig, which researchers have long believed to be working in service of the Iranian government. So far, the leaker or leakers have published a collection of the hackers' tools, evidence of their intrusion points for 66 victim organizations across the world, the IP addresses of servers used by Iranian intelligence, and even the identities and photographs of alleged hackers working with the OilRig group.

"We are exposing here the cyber tools (APT34 / OILRIG) that the ruthless Iranian Ministry of Intelligence has been using against Iran's neighboring countries, including names of the cruel managers, and information about the activities and the goals of these cyber-attacks," read the original message posted to Telegram by the hackers in late March. "We hope that other Iranian citizens will act for exposing this regime's real ugly face!"

The exact nature of the leaking operation and the person or people behind it are anything but clear. But the leak seems intended to embarrass the Iranian hackers, expose their tools—forcing them to build new ones to avoid detection—and even compromise the security and safety of APT34/OilRig's individual members. "It looks like either a disgruntled insider is leaking tools from APT34 operators, or it's a Shadow Brokers–esque sort of entity interested in disrupting operations for this particular group," says Brandon Levene, head of applied intelligence at the security firm Chronicle, which has been analyzing the leak. "They do seem to have something out for these guys. They're naming and shaming, not just dropping tools."

As of Thursday morning, the Read My Lips leakers continued to post names, photos, and even contact details of alleged OilRig members to Telegram, though WIRED couldn't confirm that any of the identified men were actually connected to the Iranian hacker group. "From now on, we will expose every few days the personal information of one of the cursed staff and secret information from the vicious Ministry of Intelligence so to destroy this betraying ministry," a message posted by the leakers on Thursday read.

Chronicle's analysts confirm that at least the hacking tools released are in fact OilRig's hacking tools, as the leakers claimed. They include, for instance, programs called Hypershell and TwoFace, designed to give the hackers a foothold on hacked web servers. Another pair of tools called PoisonFrog and Glimpse appear to be different versions of a remote-access Trojan called BondUpdater, which researchers at Palo Alto Networks have observed OilRig using since last August.

Beyond leaking those tools, the Read My Lips leaker also claims to have wiped the contents of Iranian intelligence servers, and posted screenshots of the message it says it left behind, like the one shown below.

When the Shadow Brokers spilled their collection of secret NSA hacking tools over the course of 2016 and 2017, the results were disastrous: The leaked NSA hacking tools EternalBlue and EternalRomance, for instance, were used in some of the most destructive and costly cyberattacks in history, including the WannaCry and NotPetya worms.

Read the rest here:

https://www.wired.com/story/iran-hackers-oilrig-read-my-lips/

Membership Corner

Membership Update

The 2019 Fellows cycle is now open! The Fellows Program formally recognizes significant contributions to the cyber community, cyber profession, ISSA leadership and sustained ISSA membership. The elite status of Distinguished Fellow designation is limited to only 1% of ISSA members and Fellow status is limited to 2% of the ISSA membership. Senior Membership is also an option. Information about the requirements and how to apply can be found on the ISSA International website at https://www.issa.org/page/FellowProgram (see Page 8 in this newsletter.)

Nominations and applications are received on an annual cycle and for 2019 will be accepted through June 17, 2019. Following the application period, there will be a ten-week applicant review period by the independent Fellows Committee. The committee will provide a slate of qualified applicants to the ISSA Board of Directors for consideration of being inducted into the Fellows program. The newly selected Distinguished Fellows and Fellows will be initiated at the 2019 ISSA International Conference.

In 2018 Colorado Springs added one Distinguished Fellow, Glenn York, and two Fellows, Wally Magda and Shawn Murray. If, after reviewing the requirements for Distinguished Fellow, Fellow or Senior Member, you believe you meet the criteria and are interested in submitting a package please contact Dave Reed at membership@issa-cos.org or any board member at cos-board-new@issa-cos.org.

New Members April
Nigel Webb
Beau Anglado
Timothy Pettigrew
Annie Song
Thomas Giles

Our membership is holding at ~460 members as of the end of April. 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.

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,

David Reed

Membership Committee Chairman

membership@issa-cos.org

New Chapter By-Laws have been posted on the ISSA-COS website and may be found here:

https://issa-cos.org/wp-content/uploads/2018/12/Colorado-Springs-ISSA-ByLaws-FINAL-Dec-2018.pdf

Murphy's Law: Apps To Die For

By Staff, StrategyPage, May 3, 2019

Despite its poverty and increasingly unreliable electricity supply North Korea has eagerly adopted the cell phone, often for uses the government forbids. For example, North Korea tried to keep forbidden media (South Korean and Chinese videos and music) off North Korean cell phones by installing a tracking and authentication software on North Korean smartphones (the only ones most North Koreans could own). This app was mandatory and police can check for it any time they want. If the app is not there you go to prison camp or pay the cop a large bribe.

Over the last few years, there have been a growing number of illegal apps developed by North Koreans to enable cell phone users to put forbidden media on their phones and play it without getting caught. This should not come as a surprise because North Korea has developed a formidable force of government trained hackers since the 1990s. A growing number of the official and unofficial (self-taught) hackers have secretly developed cell phone apps for all sorts of tasks, not just ones that circumvent the tracking and media access features of North Korean cell phones. These illegal apps also include stealth features that make it difficult for police to easily find that a phone has illegal media and tracking avoidance apps installed. There is an economic incentive for this because the police quickly found that they could make a lot of money by taking bribes from people caught with foreign content and illegal apps on their cell phones or any evidence that the cell phone was equipped to carry out an illegal task.

Police are supposed to seize cell phones found to contain illegal apps and content. Police quickly found that it was better for them if they took the bribe instead. Police could get away with this by meeting their quota of arrests and confiscations while waiting for the next bribery jackpot. For cell phone owners the bribe was potentially a matter of life or death. Labor camps are unhealthy places to be and spending a few years in one carries a high risk (30 percent or more depending on age and health) of death.

Officially the government is appalled at the persistence and spread of this illegal cell phone use. Privately, government officials are well aware of what is actually going on and can't officially admit that the presence of cell phones, forbidden media and the spread of legal free markets (creating more North Koreans who can afford to pay bribes if caught) is undermining the control the government once exercised over the population. Worse, many of the cell phone pirates are children of the senior officials. That's the one percent of the population that keeps the police state going. Occasionally the government will make an example of one of these ruling class kids caught with illegal content. But such punishment is bad for the morale of the key families and cannot be used frequently. The fact that such misbehavior persists and thrives is a sign that the North Korean police state is in trouble with no solution in sight. The fact is that cell phones have become essential items in North Korea and there is no going back on that.

Cell phone ownership rapidly increased over the last decade. At first, only a few thousand legal and many more illegal (Chinese) cell phones were in use. Now 70 percent of households have at least one cell phone and over four million cell phones are in use and about a quarter of those are illegal. The primary use of cell phones is communication, given the lack of private landline phones for most North Koreans and the unreliable electricity supply. North Korean users found that they by keeping their cell phones charged they would still have service during the increasingly frequent periods when there was no power. The growing use of solar panels by North Koreans is mainly for keeping the cell phones charged and a few electronic items working during power outages.

After long resisting the introduction of the more powerful smartphones North Korea finally relented in 2013. That was when North Korea announced that it had designed and begun manufacturing a smartphone (using the Android operating system). Foreign experts believed this was another publicity stunt and that the phones were actually manufactured to order from one of the many Chinese firms that do this. That proved to be the case and North Korea has never developed much of a local consumer electronics manufacturing capability. There are plenty of Chinese manufacturers willing to do the job cheaper than North Korea could manage. The North Korean smartphones are modified to make it more difficult for users to do unauthorized things like make international calls, access the Internet outside North Korea or use unauthorized apps. North Korea allows these phones to freely download approved apps, videos and music. By 2015 North Korea announced that users could download a digital version of a boring state-run publication; Rodong Sinmun. The only people who download it are government officials who believe it would be a mistake not to. The most popular downloads were illegal. Yet because the state monitors what is downloaded onto these smartphones an underground industry to provide illegal apps to get forbidden content on North Korean cell phones soon emerged. Much of the work on creating and distributing these illegal apps is done by volunteers, some of them state trained professional hackers. This is a truly disturbing development. It shows that in some ways North Korea is just like the more affluent developed nations. For North Korean leaders this is a very disturbing development.

Read the rest here:

https://www.strategypage.com/htmw/htmurph/articles/20190503.aspx

(Continued from page 1)

traditional DoD community will also be well represented but, ISSA-COS is working to expand our intelligence into non-DoD industries. So please, invite your healthcare providers, your financial institutions, your family's educators, and your retail stores of choice. Help us create a safer community for us to work, play, and live in. Registration will for Peak Cyber will soon open. When it does, be sure to register early and often.

As always, on behalf of our Board of Directors and Key Personnel, I thank you for your support and participation. Your membership helps make our chapter one of the most effective and industry relevant chapters in the world.

Sincerely,

Ernest

A Note From Our President

United Airlines covers up seat cameras to respond to privacy concerns

By Pierluigi Paganini , Security Affairs, April 29, 2019

Flying on United Airlines planes it is possible to find cameras included in screen and entertainment products used by the airline and mounted in the back of the seats. "A viral photo showing a camera in a Singapore Airlines in-flight TV display recently caused an uproar online." reported BuzzFeed. "The image was retweeted hundreds of times, with many people expressing concern about the privacy implications. As it turns out, some seat-back screens in American Airlines' premium economy class have them, too."

In response to user privacy concerns, the airline decided to cover every camera in entertainment systems, but pointed out that their purpose was not the surveillance of the passengers.

A company spokesman announced that the cameras will now be covered.

The company explained that the presence of the cameras could open for future applications for business and entertainment (i.e. gaming, video conferencing).

"As with many other airlines, some of our premium seats have in-flight entertainment systems that came with cameras installed by the manufacturer." reads a United Airlines spokesperson' statement. "None of these cameras were ever activated and we had no plans to use them in the future, however we took the additional step to cover the cameras. The cameras are a standard feature that manufacturers of the system included for possible future purposes such as video conferencing."

The company is using stickers to cover these cameras, even for all new premium seats.

Recently also Singapore Airlines was criticized for the usage of cameras under the screen with the seats pointing to the passengers.

Read the rest here:

https://securityaffairs.co/wordpress/84658/digital-id/united-airlines-seats-cameras.html

Wrecked Cars Are Now a Treasure Trove of Personal Information

By Matt Posky, The Truth About Cars, April 1, 2019

As cars grow more dependent upon computer-controlled driving aids and automakers implement permanent internet connectivity, we've grown increasingly concerned with how automakers handle their customer's data.

It sounds conspiratorial, but there's a series of events to hang the tinfoil hat on. In 2017, General Motors announced it had successfully monitored the listening habits of 90,000 motorists in a study aimed at improving marketing insights. It also rejiggered OnStar and introduced the Marketplace app for seamless in-car purchasing options. Our take was that it was as impressive as it was ominous — and GM is only leading the charge into a what analysts believe will eventually become a multi-billion dollar industry.

Naturally, this led to privacy concerns over how automakers will protect customer data on future models. But we might want to start worrying about the cars we have now. A couple of white-hat hackers (those are the good ones) recently probed the internal computer networks of wrecked and salvaged Teslas and found a mother lode of personal information waiting inside.

Read the rest here:

https://www.thetruthaboutcars.com/2019/04/wrecked-cars-are-now-a-treasure-trove-of-personal-information/

MEET THE BOARD MEMBER

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

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

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

I joined (ISSA) (COS) in 2005 and have been a member for nearly 14 years.

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

After a few of years as a Chapter member, an opportunity to become a Member at Large opened and I was accepted. Part of being on the board is to pay it forward and give back to the Chapter and profession.

Tell us something about yourself?

Being a shy introvert and a lefty in a right handed Type A world, talking about yourself is not high on the list of things to do, but I am working on it. When I get a chance, I like to go to the mountains and play golf (work in progress).

What is your experience in the Information Systems security arena?

I have been in IA/Cyber for nearly 18 years. I started out with Computer Science (CSC) as a System Engineer working IA projects and supporting Boeing on GPS. Later moving to Boeing as Lead Information Systems Security Engineer (ISSE) and Subject Matter Expert (SME) supporting GPS for 10 years. At Parsons I was a Principal IA SETA Engineer supporting the Information Assurance Manager (IAM) and the Chief IA Engineer for the Command, Control, Battle Management and Communications (C2BMC) element of the Ballistic Missile Defense System (BMDS) for the Missile Defense Agency (MDA). At NDP, LLC/Gnostech, Inc. I was an_Information Assurance Engineer supporting the Satellite Control Network Contract (SCNC) project and Launch/Early Orbit, Anomaly Resolution, and Disposal Operations (LADO) and SBIRS projects. With CGI Federal I was a Senior System Security Engineer/Project Lead and Site management lead for CGI Federal's NORAD-NORTHCOM Primary Node Network (PNN) RMF effort. Managed customer relationships, work initiatives and program activities at all organizational levels. With Oasis/Odyssey I am a Senior Cybersecurity Engineer providing Cyber Security support to the Major Command (MAJCOM) Communication Coordination Center (MCCC) program office.

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

Instead of horror stories, I like to call them chances to excel. Most issues come down to lack of good communication. I had two developers a number of years ago that wanted to use the very latest (not government approved at the time) software. After talking to them by chance, it was clear it had not been requested or approved by the customer. The response was, the customer will like it when they see it. Needless to say, the new software was not fielded.

How has the Chapter help/supported you?

The chapter has always been a place one can go and talk to and interface with like-minded folks, a resource to tap into with questions. Someone in the chapter most likely has experienced a similar issue and can provide input and guidance at a high level. Mentoring whether formal or informal is always available.

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

The Chapter has been in continuous operation for over 25 years and first and foremost exists to serve the members. Any new or proposed expanded functions/efforts to be undertaken by the Chapter should be assessed for value to the Chapter members (personal and career wise). Outreach and collaboration with local communities and other organizations has increased in the last few years and should continue. Highlighting ISSA-COS as a valued asset to engage with and be the go to Cyber Security Organization in Colorado Springs needs to continue.

Scott has served as a Member at Large, Chapter VP and current Executive Vice President and can be reached via email at execvp@issa-cos.org, and I can be reached at vp@issa-cos.org

Mike Crandall

ISSA-COS Vice-President

Platinum Sponsor—Murray Security Services—
https://www.murraysecurityservices.com/

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Aero Sponsor—CT Cubed
https://www.ctcubed.com/

ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

Blue Ribbon Trophies & Awards
245 E Taylor St (behind Johnny's Navajo Hogan on North Nevada)
Colorado Springs
(719) 260-9911

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

ISSA Fellow Program

2019 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 500 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, please contact Jorden Smith at jordenbsmith96@gmail.com to coordinate the process. Erik is the chair of the chapter awards committee and will 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 until **June 17, 2019 at 5:00pm Eastern Time**. 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 2018 ISSA International Conference.

Familiarize yourself with the Fellow Program, and the submission guidelines. If you have questions, contact Jorden or The ISSA Fellow Manager or call 866-349-5818 (US toll free) extension 4082.

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, please feel free to use this **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.

Click here to access the Senior Member application.
Click here for the Senior Member endorsement form.

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. Please contact Erik and become familiar with the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

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.

Click here to access the Fellow application.
Click here to nominate a Fellow.
Click here to submit a Fellow letter of recommendation.

(Continued on page 9)

(Continued from page 8)

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.

Click here to access the Distinguished Fellow application.
Click here to nominate a Distinguished Fellow.
Click here to submit a Distinguished Fellow letter of recommendation.

Please help us identify candidates that we can recognize in our chapter! Please contact:

Jorden Smith

Recognition Committee Chair
jordenbsmith96@gmail.com

Report: Weaponized PDFs on the Rise

By Brandi Vincent, NextGov, April 19, 2019

Security experts have reported a substantial increase in the number of weaponized PDFs being sent largely to recipients in the United States and Britain—most of which seem to be originating in Russia.

Through all of 2018, network security company SonicWall discovered more than 47,000 new attack variants within PDF files. But in March 2019 alone, 73,000 PDF-based attacks were discovered, according to a report released Thursday.

SonicWall's President and CEO, Bill Conner, told *Nextgov* the company saw a rise in threats originating in PDFs in December and January—but by March—"It was just like, 'Woah!' It was really off the charts," he said. Conner added that many of the threats "are emanating from Russia."

Conner said that in March, the company's "Real-Time Deep Memory Inspection" technology identified more than 83,000 "never-before-seen or identified" malicious events. Of those, 67,000 were PDFs linked to scammers and more than 5,500 were PDFs with direct links to other malware. PDF is the acronym used to refer to Portable Document Format. The file format was developed in the 1990s to maintain the aesthetic of an original document's text and images that can be viewed across many programs and computer systems.

"I don't want to be the alarmist here, but clearly, our businesses and governments run on PDFs today," Conner said.

Many traditional security controls cannot yet identify or mitigate links hidden inside PDF files. Conner said the new threats are predominantly fraud, scam or phishing-style documents that look realistic now, but they could evolve into something even more dangerous in the future.

"Think of it as a spam email. It looks legit, right, so you go to click on it and you might be infected immediately or you might be infected later when it detonates. It's very sophisticated in terms of that capability," Conner said. "And just because they are using that exploit to target fraud today, doesn't mean that that exploit can't be used for other purposes later."

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/04/report-weaponized-pdfs-rise/156431/

China Exploits Fleet of U.S. Satellites to Strengthen Police and Military Power

By Brian Spegele and Kate O'Keeffe, Wall Street Journal, April 23, 2019

Orbiting 22,000 miles above Earth, a fleet of American-built satellites is serving the Chinese government in ways that challenge the U.S.

Nine of these satellites have been part of efforts to connect Chinese soldiers on contested outposts in the South China Sea, strengthen police forces against social unrest and make sure state messaging penetrates far and wide, according to corporate records, stock filings and interviews with executives. A tenth satellite, under construction by Boeing Co. , would enhance China's competitor to the U.S. Global Positioning System. Besides civilian uses, the navigation system could help China in a potential conflict, such as in guiding missiles to their targets.

U.S. law effectively prohibits American companies from exporting satellites to China, where domestic technology lags well behind America's. But the U.S. doesn't regulate how a satellite's bandwidth is used once the device is in space. That has allowed China to essentially rent the capacity of U.S.-built satellites it wouldn't be allowed to buy, a Wall Street Journal investigation found.

Tangled webs of satellite ownership and offshore firms have helped China's government achieve its goals. Some of America's biggest companies, including private-equity firm Carlyle Group in addition to Boeing, have indirectly facilitated China's efforts, the Journal found.

All this appears to run counter to the U.S.'s stance of confronting China's military buildup and condemning what international watchdog groups describe as widespread human-rights abuses by China's police. That includes in far-flung territories, where the satellites help the government beam communications. Current and former U.S. officials who reviewed the Journal's findings called the satellite deals worrisome examples of China using U.S. commercial technology for strategic gain.

"It's a serious ethical and moral problem as well as a national-security issue," said Larry Wortzel, a former chairman of the bipartisan U.S.-China Economic and Security Review Commission, a group that advises Congress.

Boeing, in response to questions, said it has put on hold its latest satellite deal involving China, the one that would bolster the Chinese rival to GPS. Boeing said it complies with all U.S. laws, as did Carlyle.

China and the U.S. are locked in a battle to dominate the world's top technologies, such as biotech, chips and communications. U.S. officials say Beijing at times turns to espionage and cyberhacking to achieve its goals. In other cases, such as in the commercial satellite industry, it creatively sidesteps U.S. regulations and leverages American companies' eagerness for revenue to reap the benefits of the technology it needs to further its strategic goals.

The Chinese satellite workaround has persisted for years. U.S. officials and industry players have said the profits American satellite exports generated could be reinvested in development to keep the U.S ahead. Some defense officials also said China's use of U.S. satellites gave Washington valuable insight into its rival's space capabilities. They assumed China would use U.S.-built satellites for benign purposes such as broadcasting sports.

A Hong Kong company called Asia Satellite Telecommunications Co. has long been a bridge between mainland China and U.S. satellite makers. AsiaSat is jointly controlled by Citic Group—a conglomerate owned by China's central government—and Carlyle, which together own about 75% of the firm.

Read the rest here:

https://www.wsj.com/articles/china-exploits-fleet-of-u-s-satellites-to-strengthen-police-and-military-power-11556031771

2019 Schedule of Events

Chapter Meetings – Dinner

Tuesday, May 21, 2019

Tuesday, July 16, 2019

Tuesday, August 20, 2019

Tuesday, October 15, 2019

Tuesday, November 19, 2019

Chapter Meetings – Lunch

Wednesday, May 22, 2019

Wednesday, July 17, 2019

Wednesday, August 21, 2019

Wednesday, October 16, 2019

Wednesday, November 20, 2019

Mini-Seminars

Saturday, May 25, 2019

Saturday, July 20, 2019

Saturday, August 24, 2019

Saturday, October 19, 2019

Saturday, November 23, 2019

Special Interest Group Gatherings

Thursday, June 20, 2019

Thursday, September 5, 2019

Thursday, December 5, 2019

ISSA-COS Conferences

Peak Cyber

Tuesday, September 3, 2019

Wednesday, September 4, 2019

Thursday, September 5, 2019

Quarterly Recognition & Networking Events

Tuesday, June 18, 2019

Tuesday, September 3, 2019

Thursday, December 5, 2019

Security +CE Reviews

Saturday, September 14, 2019

Saturday, September 21, 2019

Saturday, September 28, 2019

CISSP Review

Friday, June 7, 2019

Saturday, June 8, 2019

Saturday, June 15, 2019

Friday, June 21, 2019

Saturday, June 22, 2019

Saturday, June 29, 2019

Annual Award Ceremony

Thursday, December 5, 2019

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

Automated Racism: Chinese Police Are Reportedly Using AI to Identify Minority Faces

By Melanie Ehrenkranz, Gizmodo, April 15, 2019

Facial recognition technology can target entire populations of a specific demographic, and in the wrong hands, can be used as a powerful tool for discrimination. In China, this isn't a cautionary tale, it's already happening.

According to a report from the New York Times published on Sunday, the Chinese government is using a facial recognition system to track Uighurs, the country's Muslim minority. The technology reportedly targets this population based on their physical appearance.

According to government procurement documents obtained by the Times, beginning last year, nearly two dozen police departments in China wanted technology that could identify and track Uighur individuals. And the documents reportedly indicate that the interest in this type of tech has grown in the last two years. In Yongzhou, for instance, police wanted software that could "characterize and search whether or not someone is a Uighur."

The technology is reportedly being deployed across the country, including in Hangzhou, Wenzhou, Fujian, and Sanmenxia. In Sanmenxia, police reportedly identified Uighur residents 500,000 times in just a month, starting February of this year. The database for this facial recognition system reportedly included tags for "rec_gender", "rec_sunglasses" and "rec_uygur". The latter tag was meant to indicate whether a camera identified a Uiguir, which reportedly happened 2,834 times and included images with the entry.

In China, the Uighur population is treated with suspicion and oppression by the Communist Party and is heavily surveilled by authorities. Many Uighurs have disappeared into internment camps, last year watchdogs estimated that up to a million people could be incarcerated in these specially designed prisons.

"I don't think it's overblown to treat this as an existential threat to democracy," Jonathan Frankle, an A.I. researcher at the Massachusetts Institute of Technology, told the New York Times. "Once a country adopts a model in this heavy authoritarian mode, it's using data to enforce thought and rules in a much more deep-seated fashion than might have been achievable 70 years ago in the Soviet Union. To that extent, this is an urgent crisis we are slowly sleepwalking our way into."

The use of widespread surveillance tools is far from uncommon in China—authorities in the country already monitor the location of alternative energy vehicles, the real-time moods of students in class, and citizen's "social credit" scores. And these barely factor in the existing nearly 200 million cameras in the country used for surveillance. And last year, cops in the country literally wore facial recognition systems on their face in the form of smart glasses. The stated purpose was to spot fugitives, but skeptics believed they would be misused to target activists and minorities.

Read the rest here:

https://gizmodo.com/automated-racism-chinese-police-are-reportedly-using-a-1834054068

Update Your Profile!

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

SPECIAL INTEREST GROUPS (SIGS)

Special Interest Groups (SIGs) are groups comprised of Cybersecurity professionals who gather together to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: Affinity Groups and Industry Groups. On a quarterly basis, ISSA-COS brings together both groups to participate in formally structured events. During these gatherings, participants have an opportunity to first attend one of four (4) Affinity Groups then, one of four (4) Industry Groups. CPEs/CPUs are awarded for attend these events.

In-between formal gatherings, the SIG Leaders for each individual SIG are encouraged to coordinate informal gatherings. ISSA-COS encourages SIG leaders to consider hosting informal gatherings at social venues such as sporting events, restaurants, bars, or breweries. Informal gatherings may also include participating in a community improvement project, a group walk or hike, or a picnic/BBQ.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups gather to share security related experiences, impart knowledge and education, and help one another solve common problems and issues. The Affinity Groups currently promoted by ISSA-COS include:

Women in Security – **W***[omen]***IS**

Young Professional in Security – **Y***[oung Professionals]***IS**

Mentoring in Security – **M***[entoring]***IS**

Executives in Security – **E***[xecutives]***IS**

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups gather together to discuss security related topics and share solutions to problems affecting their perspective industries. They also exchange Cybersecurity related tips, information, and education specific to their industries. The Industry Groups currently promoted by ISSA-COS include:

Finance in Security – **F***[inance]***IS**

Healthcare in Security – **H***[ealthcare]***IS**

Retail in Security – **R***[etail]***IS**

DoD in Security – **D***[oD]***IS**

ISSA-COS invites you to join us at our next SIG gathering or any one of our many other events.

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

There's a massive cybersecurity job gap – we should fill it by employing hackers

By John McAlaney and Helen Thackray, Homeland Security News Wire, April 17, 2019

Cybersecurity incidents are gaining an increasingly high profile. In the past, these incidents may have been perceived primarily as a somewhat distant issue for organizations such as banks to deal with. But recent attacks such as the 2017 Wannacry incident, in which a cyber attack disabled the IT systems of many organizations including the NHS, demonstrates the real-life consequences that cyber attacks can have.

These attacks are becoming increasingly sophisticated, using psychological manipulation as well as technology. Examples of this include phishing emails, some of which can be extremely convincing and credible. Such phishing emails have led to cybersecurity breaches at even the largest of technology companies, including Facebook and Google.

To face these challenges, society needs cybersecurity professionals who can protect systems and mitigate damage. Yet the demand for qualified cybersecurity practitioners has quickly outpaced the supply, with three million unfilled cybersecurity posts worldwide.

So it might come as a surprise that there is already an active population with a strong passion for cybersecurity – hackers. This is a term with many negative connotations. It evokes the stereotypical image of a teenage boy sat in a dark room, typing furiously as green text flies past on the computer monitor, often with the assumption that some criminal activity is taking place. The idea of including such individuals in helping build and protect cyber systems may seem counterintuitive.

Read the rest here:

http://www.homelandsecuritynewswire.com/dr20190417-there-s-a-massive-cybersecurity-job-gap-we-should-fill-it-by-employing-hackers

NIST's Ron Ross on the state of cyber: 'We literally are hemorrhaging critical information'

By Jill Aitoro, Fifth Domain, March 29, 2019

After Chinese hackers infiltrated a Navy subcontractor's computer network and stole a trove of highly sensitive data on submarine warfare, it spurred the government to revise the standards that contractors must follow to ensure government data is properly protected data.

What the hackers took was "the equivalent of the stealth technology for the Air Force," said Ron Ross, a fellow at the National Institute of Standards and Technology who focuses on computer security.

"We literally are hemorrhaging critical information about key programs," Ross said during a fireside chat I moderated at the RSA Federal Summit Tuesday. "They're coming after you every day. They're either going to bring down your capability, they're going to steal stuff from you, or they're going to plant malicious code in your systems and they're going to come back at some point under their timetable and bring you down."

As for the revision of those standards, it's currently parked in the Office of Management and Budget awaiting approval, Ross said. Ideally, the Defense Department would begin to use those standards within the next 18 months to help determine whether to award a business a contract.

Read the rest here:

https://www.fifthdomain.com/dod/2019/03/29/nists-ron-ross-on-the-state-of-cyber-we-literally-are-hemorrhaging-critical-information/

The Air Force Has a New Cyber Security Defense Plan

By Kris Osborn, The National Interest, April 4, 2018

The Pentagon is having trouble bringing on cyber workers through the Cyber Excepted Service, thanks to too few personnel and a backlogged and complicated security clearance process.

The Air Force is refining new cloud-oriented cybersecurity technologies to safeguard vulnerable data networks and strengthen defenses against increasingly sophisticated AI-enabled cyber attacks.

Air Force cloud migration, designed to reduce a hardware footprint, enable broader data access and engender greater levels of combat interoperability, is seeking to benefit from various technical upgrades to keep pace with fast-evolving new cyber threats. This includes development of multi-mode authentication techniques, software-reliant network upgrades, new patches and new cyber defenses fortified by the latest AI-related innovations.

“In preparation for the cloud migration process, we put systems through intense scrutiny and analysis to determine how and if they should be modernized to meet the needs of a new Digital Air Force,” Maj. William “Bryan” Lewis, Air Force spokesman, told Warrior Maven.

Lewis added that emerging security approaches will “deploy tools, tactics, and techniques to counter AI as well as conventional cyberspace attack methods.”

AI-driven cyberattacks present a new sphere of risks for data networks because they can launch massive amounts of attacks at one time and, of even greater consequence, find vulnerabilities faster by virtue of an ability to gather, interpret, organize and analyze network defenses.

Among other things, migration to the commercial cloud removes barriers to combat-relevant information sharing in real time by reducing a need for stovepiped servers and networks -- and instead enabling instant access across otherwise disparate networks, databases and information systems.

For example, cloud access could allow an Air Force pilot to access needed additional intelligence to inform targeting, mission planning or other time-sensitive information. By extension, utilizing AI would not only facilitate rapid access to otherwise separate networks and hardware systems, but also perform real-time analytics designed to organize and deliver information against historical volumes of data. This, naturally, massively streamlines mission effectiveness.

“The Air Force is benefitting from a reduction of operations complexity and the costs associated with moving to commercial cloud solutions. From a combat operations vantage point, getting to the cloud means the Air Force is less impacted by points of failure,” he explained.

In effect, Lewis here refers to what might be called a “double-edge” sword, or duality, meaning that cloud-migration brings both security advantages and challenges. The cloud can increase security because many nodes will still be operational and accessible should one particular entry point be compromised. Yet, singular points of entry might run the risk of exposing an attacker to a wider swath of information to steal. Cloud migration can also benefit from many protective measures extending far beyond “perimeter security” and, by virtue of increased virtualization, patch, protect or upgrade across entire networks with one “fix.”

An interesting 2012 essay, called “Addressing Cloud Computing Security Issues,” seems to anticipate this evolving predicament, namely that maximizing access through cloud applications can accentuate vulnerabilities. However, the essay -- from a text called “Future Generation Computer Systems” -- also states that the “homogeneous resource pooled nature of the cloud” can allow for far-reaching applications of security procedures.

For instance, the point raised in the essay aligns with some of the concepts inspiring DoD’s accelerated cloud migration and move to Windows 10. Underway now for several years, the Pentagon’s ongoing move to Windows 10 is, by design, intended to enable networks to quickly access the most current patches and security "fixes" made necessary by emerging threats.

“One of the biggest risks is an unpatched old windows server in the cloud. The cloud is, by nature, characterized by accessibility...you can access it anywhere…. which creates the challenges,” Sean Frazier, Federal CISO, Duo Security Business Unit, Cisco, told Warrior Maven in an interview.

Also, when it comes to cloud operations, growing use of AI and automation can lead toward more real-time analytics, identifying anomalies more quickly and reaching entire networks quickly with new virtualized, or software-driven security enhancements.

Read the rest here:

https://news.yahoo.com/air-force-cyber-security-defense-094400968.html

Are keyloggers recording you?

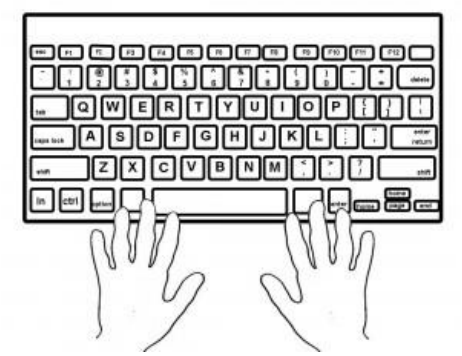
By Staff, Malware Bytes Newsletter, April, 2018

What is a keylogger?

Did you know that your keyboard could let cybercriminals eavesdrop on you? Or that they could watch you on your system camera? Or listen over your smartphone's microphone? Welcome to the world of keyloggers, a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device.

Although for our purposes, keyloggers operate in the context of malware, they are not always illegal to install and use. Keyloggers are a common tool for corporations, which information technology departments use to troubleshoot technical problems on their systems and networks—or to keep an eye on employees surreptitiously. The same goes for, say, parents, who want to monitor their children's activities. Suspicious spouses are another market for keyloggers.

In all such cases, if the organization or person downloading and installing the keylogger actually owns the device, then it's perfectly legal. And there are thousands of commercially available keyloggers on the Internet, which advertise themselves for just such a use.



However, the concern about keyloggers is when malicious actors are behind them. And they definitely do not own the device they infect. You don't know they've breached your computer; and depending on what kind of keylogger it is, it can steal any passwords you've entered, periodically take screen shots, record the web pages you view, grab on to your sent emails and any instant messaging sessions, as well as sensitive financial information (such as credit card numbers, PIN codes, and bank accounts), and then send all that data over the network to a remote computer or web server. There, the person operating the logging program can retrieve it all, no doubt sending it to third parties for criminal purposes.

Keyloggers come in at least two broad flavors—hardware devices and the more familiar software variety. Hardware devices can be embedded in the internal PC hardware itself, or be an inconspicuous plugin that's secretly inserted into the keyboard port between the CPU box and the keyboard cable so that it intercepts all the signals as you type. But that means that the cybercriminal has to have physical access to the PC while you're not present in order to plant the hardware keyloggers.

Software keyloggers are much easier to introduce to and install on victims' devices, which is why that variety is much more common. Unlike other kinds of malware, software keyloggers are not a threat to the systems they infect themselves. In fact, the whole point of keyloggers is to work behind the scenes, sniffing out the keystrokes while the computer continues to operate normally. But even if they don't harm the hardware, keyloggers are definitely a threat to users, especially when they steal data pertinent to any number of online payment systems.

How can I tell if I have a keylogger infection?

Keyloggers invade PCs (and Macs, and Androids, and iPhones) in the same way that other malware does. They install when you click on a file attachment that you've been duped into opening—most commonly because you fell for a social engineering scheme or a cleverly designed phishing expedition. The attachments can come to you by email, through a text message, an instant message, on social networks, or even through a visit to an otherwise legitimate but infected website, which exploits a vulnerability in it and drops a drive-by malware download. Also, keyloggers rarely arrive solo. The same Trojan that delivers the keylogger can slip other malware on your system—such as adware, spyware, ransomware, or even a legacy virus.

"Keyloggers install when you click on a file attachment that you've been duped into opening—most commonly because you fell for a social engineering scheme or a cleverly designed phishing expedition."

Hardware keylogger infections occur if someone gains access to your unlocked device, which can fuel any number of scenarios. Say a crook somehow installs a keylogger plug into the keyboard USB port of a bank loan officer's PC. That gives the keylogger operator all kinds of exploitable data in the course of the loan officer's normal duties. Corporate accounting department computers are another rich target. Or what if you decide to use a public computer to do some shopping? The last person using that Internet café PC could be the next one to use your confidential data.

What is the history of keyloggers?

Read the rest here:

https://www.malwarebytes.com/keylogger/

Trump Signs Executive Order to Boost Federal Cyber Workforce

By Brandi Vincent, Nextgov, May 2, 2019

The White House launched its latest effort to bolster the government's cybersecurity workforce.

President Trump issued an executive order Thursday that introduces new initiatives and expands existing national efforts aimed to "grow and strengthen" America's cyber workforce. The programs laid out in the order will help better standardize cross-government language around cybersecurity, incentivize engagement from academia and federal agencies, and accelerate learning to address the nation's urgent need to fill the cyber workforce gap.

"More than 300,000 cybersecurity job vacancies exist in the United States today," President Trump said in a statement. "They must be filled to protect our critical infrastructure, national defense, and the American way of life."

Senior administration officials noted that the order begins to address the challenge of ensuring that cybersecurity professionals have mobility into and outside of federal government and industry.

"United States Government policy must facilitate the seamless movement of cybersecurity practitioners between the public and private sectors, maximizing the contributions made by their diverse skills, experiences, and talents to our Nation," the order said.

The administration is also creating a federal rotational program in which feds can expand their expertise through temporary cyber-related assignments within other agencies, in hopes that new exposure will increase skills and encourage interagency knowledge transfers. The program mirrors a bipartisan bill that the Senate passed this week, which enables some cyber professionals to rotate across various agencies.

The order establishes a "President's Cup" cybersecurity competition that will challenge and reward the government's top cyber personnel. The new competition is still in its planning process, officials said, but it's being modeled off of other national collegiate cyber contests.

Officials said the order will also help agencies identify and implement aptitude assessments that will help re-skill employees who exude potential.

The order will also introduce new awards programs that will recognize government personnel who have made significant contributions to cybersecurity or cyber operations. It will also establish the Presidential Cybersecurity Education Awards to celebrate elementary and secondary school educators teaching cybersecurity-related content.

In an effort to get government insiders on the same page around cyber practices and language, the order also encourages the widespread adoption of the National Institute of Standards and Technology's National Initiative for Cybersecurity Education, or NICE framework, which serves as a reference for identifying, recruiting, developing, and retaining cybersecurity talent.

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/05/trump-signs-executive-order-boost-federal-cyber-workforce/156709/

Now, if you are REALLY BORED!

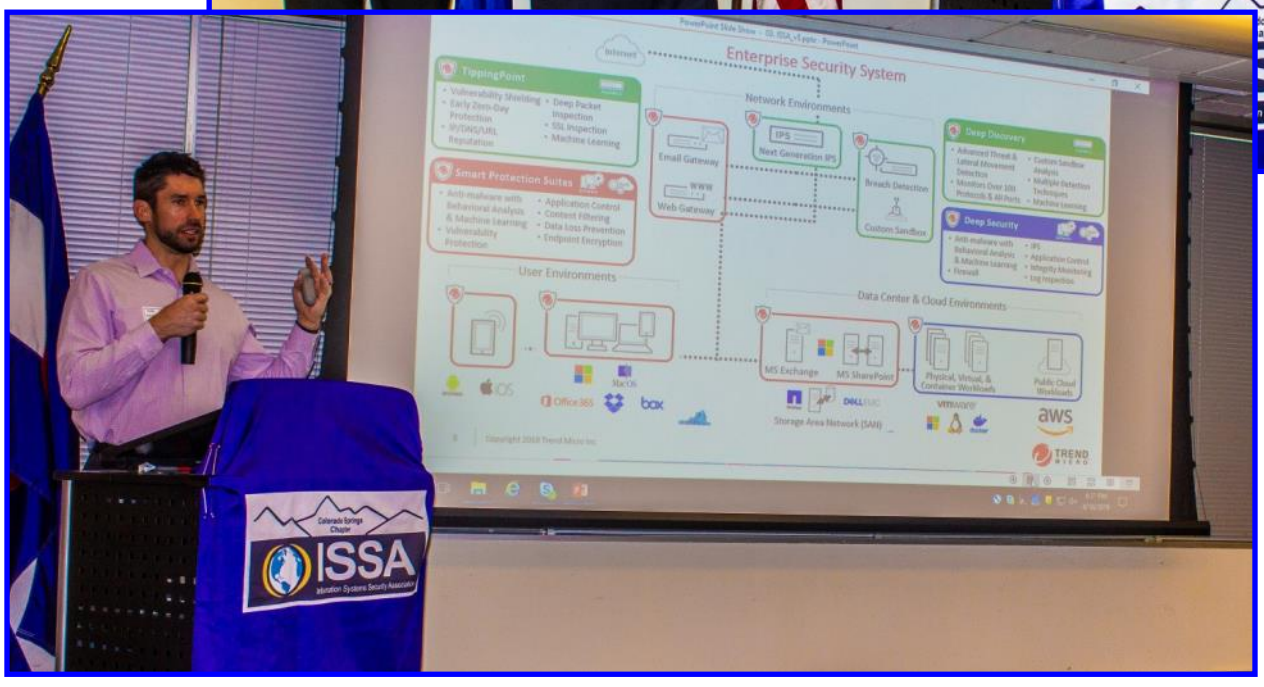
Cybersecurity Rap Song

According to the advertising blurb: "*This is a fun and educational rap song about Cyber Security that combines an upbeat song and fun graphics with tips and lessons on IT security.*" You be the judge.

https://youtu.be/b8oHN0S2biw

ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce



Additional photographs are available on the ISSA-COS.ORG *website.*

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

WWW.ISSA-COS.ORG

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

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

Article for the Newsletter?

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

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Chapter Officers:

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: Mark Maluschka
- Deputy Treasurer: Vacant

Recorder/Historian: Mike Daetwyler
- Deputy: **Vacant**

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

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: David Reed
- Deputy: Melissa Absher

Vice President of Training: Mark Heinrich
- Deputy: Jeff Tomkiewicz

Member at Large: James Asimah
Member at Large: Bill Blake
Member at Large: Jim Blake
Member at Large: **Vacant**

Committee Chairs:

Training: Mark Heinrich
Hospitality: Stephen Parish
Mentorship Committee Chair: Carissa Nichols
Ethics: Timothy Westland
Recognition: **Vacant**
Media: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

Executive Assistant: Andrea Heinz

** Executive Board Members*

Significant Interest Group Leads:

Chair: **Vacant**
Women in Security : June Shore
Young Prof. in Security: Jeremiah Walker
Educators in Security: **Vacant**
Executives in Security: **Vacant**
Finance in Security: **Vacant**
Healthcare in Security: Dennis Schorn
Retail in Security: **Vacant**
DoD in Security: Steven Mulig

Past Senior Leadership

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

Dead people 'will outnumber the living on Facebook', and it could be a problem

By Rob Waugh, Yahoo News UK, April 29, 2019

In the not too distant future, Facebook profiles for dead people will actually outnumber the living people on the site, a new study has suggested.

Within 50 years, Facebook will be like a digital graveyard, containing hundreds of millions of people – and it raises important questions over who owns the data of the dead, the researchers said.

Read the rest here:

https://news.yahoo.com/dead-people-will-outnumber-living-facebook-problem-183152738.html

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