ISSA
Information Systems Security Association
Colorado Springs Chapter

WWW.ISSA-COS.ORG

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 10

OCTOBER 2019

Autumn is *Finally* Here!

A Note From Our President

By Mr. Ernest Campos

ISSA-COS Members,

Welcome to October! The month full of sugar and spice… pumpkin spice that is! Apart from all the candy treats, October is also National Cybersecurity Awareness month. To help contribute to the focus of the month, our chapter will host a panel discussion at our chapter dinner and lunch meetings. The theme for these meetings is "**Cybersecurity in Colorado Springs: Past, Present, and Future**." We have compiled a phenomenal team of panel members from our various community partners; representatives from the city, local academia, and local/national Cyber-focused non-profits. We are anticipating a large crowd of attendees so be sure to register early.

Looking back at September, we experienced record breaking registration and attendance at the 9th Annual Peak Cyber Symposium; both for the Capture-the-Flag event and for the symposium. Looking forward to 2020 and the **10th Annual Peak Cyber Symposium**, we have great momentum for this nationally attended event. We have already started our planning process and we are prepping for a truly stellar event. In September, we also participated in the 3rd annual National Cybersecurity Center (NCC) Cyber Symposium. Our chapter posted a great booth with many visitors and we held a guest speaking spot whereby, we promoted our chapter and the value of investing in organizations like our chapter.

Also, in the month of September, we conducted the **2019 General Membership Survey**. "Thank You" to all those who participated. The results of this survey (*see pages 7 through 11*) will help shape the future of our chapter as we continue to prepare ourselves for the future of Cybersecurity in our region. Take note, the future will not resemble the past but, it will honor and learn from it. Going forward in 2020 and beyond, our chapter will complete our efforts to establish ourselves as an institution within our community. We will complete the implementation of a firm schedule of annual events, the institution of repeatable processes for conducting events,

(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.

Russia carried out a 'stunning' breach of FBI communications system, escalating the spy game on U.S. soil

By Zach Dorfman, Jenna McLaughlin and Sean D. Naylor, Yahoo News, September 16, 2019

On Dec. 29, 2016, the Obama administration announced that it was giving nearly three dozen Russian diplomats just 72 hours to leave the United States and was seizing two rural East Coast estates owned by the Russian government. As the Russians burned papers and scrambled to pack their bags, the Kremlin protested the treatment of its diplomats, and denied that those compounds — sometimes known as the "dachas" — were anything more than vacation spots for their personnel.

The Obama administration's public rationale for the expulsions and closures — the harshest U.S. diplomatic reprisals taken against Russia in several decades — was to retaliate for Russian meddling in the 2016 presidential election. But there was another critical, and secret, reason why those locations and diplomats were targeted.

Both compounds, and at least some of the expelled diplomats, played key roles in a brazen Russian counterintelligence operation that stretched from the Bay Area to the heart of the nation's capital, according to former U.S. officials. The operation, which targeted FBI communications, hampered the bureau's ability to track Russian spies on U.S. soil at a time of increasing tension with Moscow, forced the FBI and CIA to cease contact with some of their Russian assets, and prompted tighter security procedures at key U.S. national security facilities in the Washington area and elsewhere, according to former U.S. officials. It even raised concerns among some U.S. officials about a Russian mole within the U.S. intelligence community.

"It was a very broad effort to try and penetrate our most sensitive operations," said a former senior CIA official.

> *"This is, in fact, the core risk and it's right that it should be the focus. But we were neither organized nor resourced to deal with counterintelligence in networks, technical networks, electronic networks."*

American officials discovered that the Russians had dramatically improved their ability to decrypt certain types of secure communications and had successfully tracked devices used by elite FBI surveillance teams. Officials also feared that the Russians may have devised other ways to monitor U.S. intelligence communications, including hacking into computers not connected to the internet. Senior FBI and CIA officials briefed congressional leaders on these issues as part of a wide-ranging examination on Capitol Hill of U.S. counterintelligence vulnerabilities.

These compromises, the full gravity of which became clear to U.S. officials in 2012, gave Russian spies in American cities including Washington, New York and San Francisco key insights into the location of undercover FBI surveillance teams, and likely the actual substance of FBI communications, according to former officials. They provided the Russians opportunities to potentially shake off FBI surveillance and communicate with sensitive human sources, check on remote recording devices and even gather intelligence on their FBI pursuers, the former officials said.

"When we found out about this, the light bulb went on — that this could be why we haven't seen [certain types of] activity" from known Russian spies in the United States, said a former senior intelligence official.

The compromise of FBI systems occurred not long after the White House's 2010 decision to arrest and expose a group of "illegals" – Russian operatives embedded in American society under deep non-official cover – and reflected a resurgence of Russian espionage. Just a few months after the illegals pleaded guilty in July 2010, the FBI opened a new investigation into a group of New York-based undercover Russian intelligence officers. These Russian spies, the FBI discovered, were attempting to recruit a ring of U.S. assets — including Carter Page, an American businessman who would later act as an unpaid foreign policy adviser to Donald Trump's 2016 presidential campaign.

The breaches also spoke to larger challenges faced by U.S. intelligence agencies in guarding the nation's secrets, an issue highlighted by recent revelations, first published by CNN, that the CIA was forced to extract a key Russian asset and bring him to the U.S. in 2017. The asset was reportedly critical to the U.S. intelligence community's conclusion that Russian President Vladimir Putin had personally directed the interference in the 2016 presidential election in support of Donald Trump.

Read the rest here:

https://news.yahoo.com/exclusive-russia-carried-out-a-stunning-breach-of-fbi-communications-system-escalating-the-spy-game-on-us-soil-090024212.html

Membership Corner

Membership Update

There are some critical volunteer opportunities upcoming with the chapter elections coming in November. The following positions are up for election this year:

Executive Vice President
Chapter Vice President
Director of Communications
VP of Membership
Treasurer
Members-At-Large (x2)

Position descriptions can be found on the chapter website (www.issa-cos.org). Candidates are required to be general members, in good standing, current on dues, and not student members. If you're interested in serving the chapter as a board member please indicate your interest in becoming a candidate NLT midnight, Oct. 11, 2019 via the following survey site: https://www.surveymonkey.com/r/8HTSRMJ .

New Members September
Ryan Van Den Heuvel
Matthew Erler
Stephen Day
Brian Barnhart
Joshua Adams
Ryan Grimshaw
Brad Bradford
Anthia Zacarias
Perry Foster
Kayla Willeford

Next, I would 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

DOD releases unified cybersecurity standard for contractors

By Lauren Williams, FCW, September 5, 2019

A draft of the unified cybersecurity standard model Defense Department contractors must follow was just released, and a senior official wants vendors to "tear it up" in the comments.

Katie Arrington, DOD's chief information security officer for the Office of the Undersecretary of Defense for Acquisition and Sustainment, announced the release of the Cybersecurity Maturity Model Certification framework Sept. 4, during a panel discussion at the Intelligence and National Security Summit in National Harbor, Md.

The CMMC framework, which is expected to be implemented in 2020, will require any company in the DOD supply chain to become certified before it can do business.

Arrington said startups and small companies that DOD relies on for innovative solutions are the most vulnerable to cybersecurity threats in the supply chain.

Adversaries "aren't going after a Lockheed Martin, at the top prime level, they're going after the small business, that [Small Business Innovation Research awardee], that [other transaction authority firm] that's the most vulnerable," she said during the panel, adding that she hopes other federal agencies also adopt the model.

Read the rest here:

https://fcw.com/articles/2019/09/05/dod-cyber-cmmc-rules-williams.aspx

(Continued from page 1)

A Note From Our President

and a predictable quality of service for all our events; a benefit to our members and invited guests. For example, have you ever wished you could invite a guest to an ISSA-COS event without having to gain approval from a board member first? Well, in 2020 you will! Have you ever wished ISSA-COS hosted regular networking events attended by area companies, organizations, and professionals? Well, in 2020 we will! Have you ever wished ISSA-COS would make the most, best, and upmost use of chapter funds to maximize opportunities to gain CPEs/CPUs and increase your technical knowledge? Well, in 2020 we will!

All year long, our Board of Directors (BoD) have been working hard to shape the future of our organization. In addition to improving the way we operate; we have also pursued strategic partnerships with local non-profit organizations that can and will add value to our chapter right down to the individual member level. **Our goal is to make membership within ISSA-COS worth the time, effort, and money sacrificed by our members; without increasing the cost of membership.** In addition to their individual efforts, the BoD took into consideration the results of the recent General Membership Survey. The results of this survey can be found in the ISSA-COS October Newsletter. Bear in mind, the results of the survey will not result in actual changes to our chapter. Rather, the results will contribute to the decision-making processes of our BoD. Furthermore, any changes adopted by our board will not take effect until 2020.

Next, let's spend a moment focusing on the **2019 Annual Elections**. This year, the following positions are open for election.

- Executive Vice President
- President
- Chapter Vice President
- Director of Communications
- VP of Membership
- Treasurer
- Members-At-Large (x2)

Anyone interested in running for one of these positions is encouraged to express their interest via the following website: https://www.surveymonkey.com/r/8HTSRMJ. The opportunity to express an interest is open until Oct. 11th. The remainder of October will be spent advertising the candidates who expressed an interest; leading up to the actual elections in November. Ultimately, we desire the newly elected officers to be able to participate in the December Board Meeting and in the December Annual Award Ceremony.

Finally, I want to give props to the following individuals who were selected by ISSA International for specific annual awards:

- ***ISSA-COS Honor Roll and ISSA Chief Operations Officer (COO):*** *Dr. Shawn Murray*
- ***Security Professional of the Year****:* *Art Cooper*
- ***Volunteer(s) of the Year****:* *Joint – Don Creamer and Warren Pearce*
- ***Senior Member****: Phebe Swopes*

Collectively, these individuals have done great things to promote our industry, our chapter, and themselves. To all of them, I express a firm "**Thank You**" for their service and commitments to ISSA and a resounding "**Congratulations**" for their selections. Individually, you have all made significate contributions to our chapter and to your own careers.

In closing, on behalf of the BoD, I express a heartfelt expression of gratitude for all our members who, on a daily basis, elevate themselves and our industry. Day-to-day, week-in and week-out, we work to make a difference in our industry. Various results motivate our individual actions but collectively, we contribute to a communal measure of success. **Thank you for all you do!**

Sincerely,

Ernest

University of Minnesota report reveals growing threat of cyberattacks to food safety

By Staff, University of Minnesota, September 10, 2019

A new report by University of Minnesota researchers indicates cyberattacks pose a rising threat to food production and safety.

"Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing," released today by the University's Food Protection and Defense Institute (FPDI), illustrates the mounting cybersecurity risk facing the food industry and provides industry-specific guidance to keep operations safe and secure. The potential consequences of an attack on the industrial control systems used in the food industry include contaminated food that threatens public health, physical harm to workers, destroyed equipment, environmental damage, and massive financial losses for companies.

While cybersecurity is rarely recognized as a food safety issue, the systems companies use for processing and manufacturing food contain many vulnerabilities that experts believe will soon present a more appealing target for cyberattacks than industries that are more commonly affected by, and therefore better prepared for, such attacks.

"The food industry has not been a target of costly cyberattacks like financial, energy, and health care companies have," said Stephen Streng, lead author on the report. "However, as companies in those sectors learn to harden their defenses, the attackers will begin looking for easier victims. This report can help food companies learn about what could be coming their way and how to begin protecting themselves."

Researchers and manufacturers identified more than 200 industrial control system vulnerabilities in 2011, the report notes, with the number increasing each year through 2016, the end of the study period. The vulnerabilities are present in a wide variety of components from different vendors, making them difficult for companies to avoid. Many systems were designed before cybersecurity was a concern and use outdated operating systems and hard-coded passwords that allow attackers easier access to the system.

In addition to vulnerabilities in the systems themselves, many other factors contribute to the heightened risk of cyberattacks. Companies often lack knowledge about how their industrial control systems and IT systems interact and lack awareness about cyber risks and threats. Further, there is poor coordination and information-sharing among food system stakeholders. Meanwhile, the tools required to carry out a cyberattack are becoming more powerful and requiring less skill to use.

"The food industry has some characteristics that make it uniquely vulnerable to cyberattacks on its processing and manufacturing systems," Streng said. "Luckily, there's still time for companies to protect themselves."

Moving forward, the report recommends that the food industry foster stronger communications between operations technology and information technology (IT) staff, conduct risk assessments that include inventories of both industrial control and IT systems, involve staff with cybersecurity expertise in procuring and deploying new industrial control systems, and extend the existing culture of food safety and defense to include cybersecurity.

"Cyberattacks could have financially devastating consequences for the food industry, particularly among smaller companies, and in the worst case can threaten the public's health," said Amy Kircher, DrPH, director of FPDI. "We hope this report will raise awareness among food industry executives of this potentially severe risk and will inspire them to start addressing it with the same care and urgency they apply to other aspects of food safety."

FPDI, a Homeland Security Center of Excellence, protects the global food supply through research, education, and the delivery of innovative solutions, addressing vulnerabilities that could lead to catastrophic damage to public health or the economy. The institute collaborates with industry, government agencies, nongovernmental organizations, and academic stakeholders to help assure product integrity, supply chain resiliency, and brand protection throughout the food system.

To read the full report, visit z.umn.edu/FPDIcybersecurity. Learn more about the Food Protection and Defense Institute at foodprotection.umn.edu.

Women Know Cyber: 100 Fascinating Females Fighting Cybercrime

By Press Release, CyberCrime Magazine, May 21, 2019

Cybersecurity Ventures has published a new book — "*Women Know Cyber: 100 Fascinating Females Fighting Cybercrime*" — which is available on Amazon.

Women Know Cyber features cybersecurity experts from across the globe, with varying backgrounds, who stand out for protecting governments, businesses, and people from cybercrime — and for their contributions to the community.

Co-authors Steve Morgan and Di Freeze dispel the myth that women are barely represented, or wanted, in the cybersecurity field. "Women hold roughly 20 percent of cybersecurity positions today, up from estimates of 11 percent in 2013," says Morgan, founder and Editor-in-Chief at Cybersecurity Ventures.

Cybercrime will more than triple the number of job openings over the next 5 years. Cybersecurity Ventures predicts there will be 3.5 million cybersecurity job openings by 2021. "To fill the world's open security positions, we'll need to aim for 50 percent of women in cyber over the next decade," says Morgan. "While some people may view that as an overly ambitious goal, it's one that the cybersecurity industry must aim for."

"I'm so inspired by these pioneering women and encouraged by their stories," states Sylvia Acevedo in the book's foreword. "Because of out-of-the-box thinkers, innovators, and leaders like them, the fight against cybercrime is entering a new era where women are confidently adding their voices to the mix — not just creating a path for themselves, but opening up opportunities for others forging ahead in their wake," adds Acevedo, a well-known author, entrepreneur, engineer, and rocket scientist.

The women featured in the book include CISOs (chief information security officers) at Fortune 500 corporations, founders of women-owned cybersecurity companies, top data privacy experts, and security leaders at companies such as Cisco, Facebook, Google, IBM, McAfee, Microsoft, RSA, Symantec, Twitter, and others.

"I'm thrilled to be a part of this amazing group of fearless women. I hope to meet all of them someday and share our stories," says Aanchal Gupta, Head of Security, Blockchain at Facebook.

The new book is aimed at students, parents, teachers, and anyone contemplating an education or career in the cybersecurity field.

Women Know Cyber is sponsored by FutureCon Events, founded by Kim Hakim, a U.S. Navy veteran with more than two decades of experience in producing thousands of cybersecurity conferences. There are two *Women Know Cyber* book signings scheduled at FutureCon — Denver, Colo. on Jul. 31, 2019, and Boston, Mass. on Oct. 9, 2019.

Download the free PDF book here:

https://cybersecurityventures.com/wp-content/uploads/2019/05/Women_Know_Cyber.pdf

FDA warns of potential cyber vulnerabilities in internet-connected medical devices

By Maggie Miller, The Hill, October 1, 2019

The Food and Drug Administration (FDA) on Tuesday warned patients, providers and manufacturers about cybersecurity vulnerabilities in certain medical devices and health care networks.

The vulnerabilities, referred to by the agency as URGENT/11, have the potential to harm operating systems for medical devices connected to communications networks like Wi-Fi and equipment such as routers and phones.

According to the FDA, the cyber vulnerabilities could allow a remote actor to "take control" of the device, leading to a change in function, information leaks or causing the device to stop functioning.

The FDA emphasized that it had not received any reports of "adverse events" that have occurred as a result of the cyber vulnerabilities.

However, Suzanne Schwartz, the deputy director of the Office of Strategic Partnerships and Technology Innovation in the FDA's Center for Devices and Radiological Health, said in a statement that the "risk of patient harm if such a vulnerability were left unaddressed could be significant."

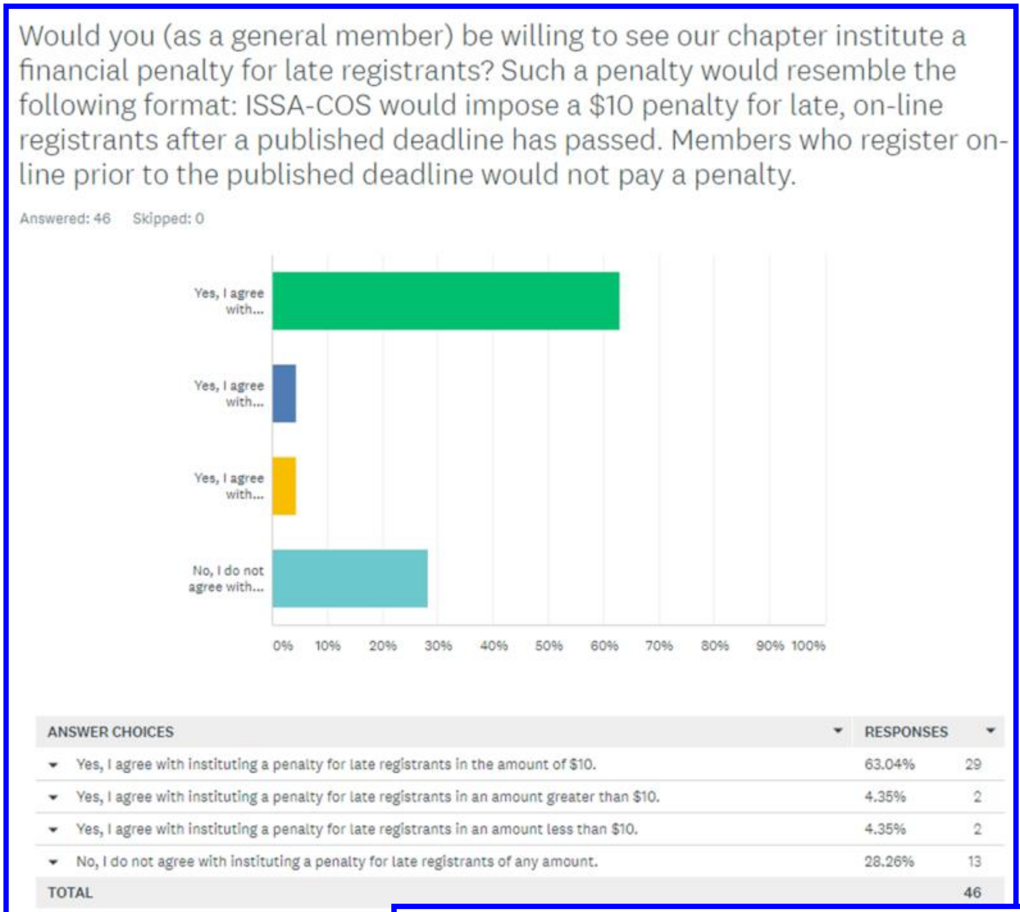
Read the rest here:

https://thehill.com/policy/cybersecurity/463914-fda-warns-of-potential-cyber-vulnerabilities-in-internet-connected

2019 General Membership Survey

-

The Results are IN!

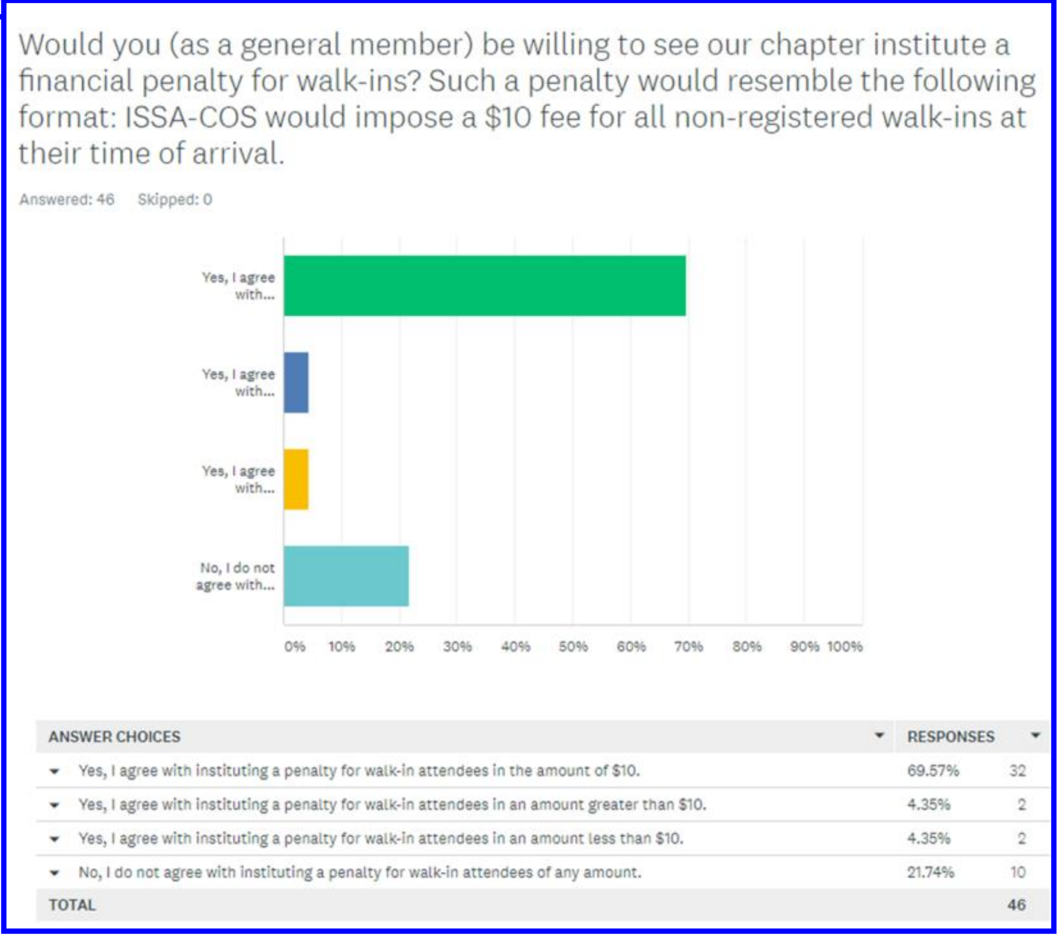


Would you (as a general member) be willing to see our chapter institute a financial penalty for late registrants? Such a penalty would resemble the following format: ISSA-COS would impose a $10 penalty for late, on-line registrants after a published deadline has passed. Members who register on-line prior to the published deadline would not pay a penalty.

Answered: 46 Skipped: 0

ANSWER CHOICES	RESPONSES	
Yes, I agree with instituting a penalty for late registrants in the amount of $10.	63.04%	29
Yes, I agree with instituting a penalty for late registrants in an amount greater than $10.	4.35%	2
Yes, I agree with instituting a penalty for late registrants in an amount less than $10.	4.35%	2
No, I do not agree with instituting a penalty for late registrants of any amount.	28.26%	13
TOTAL		46

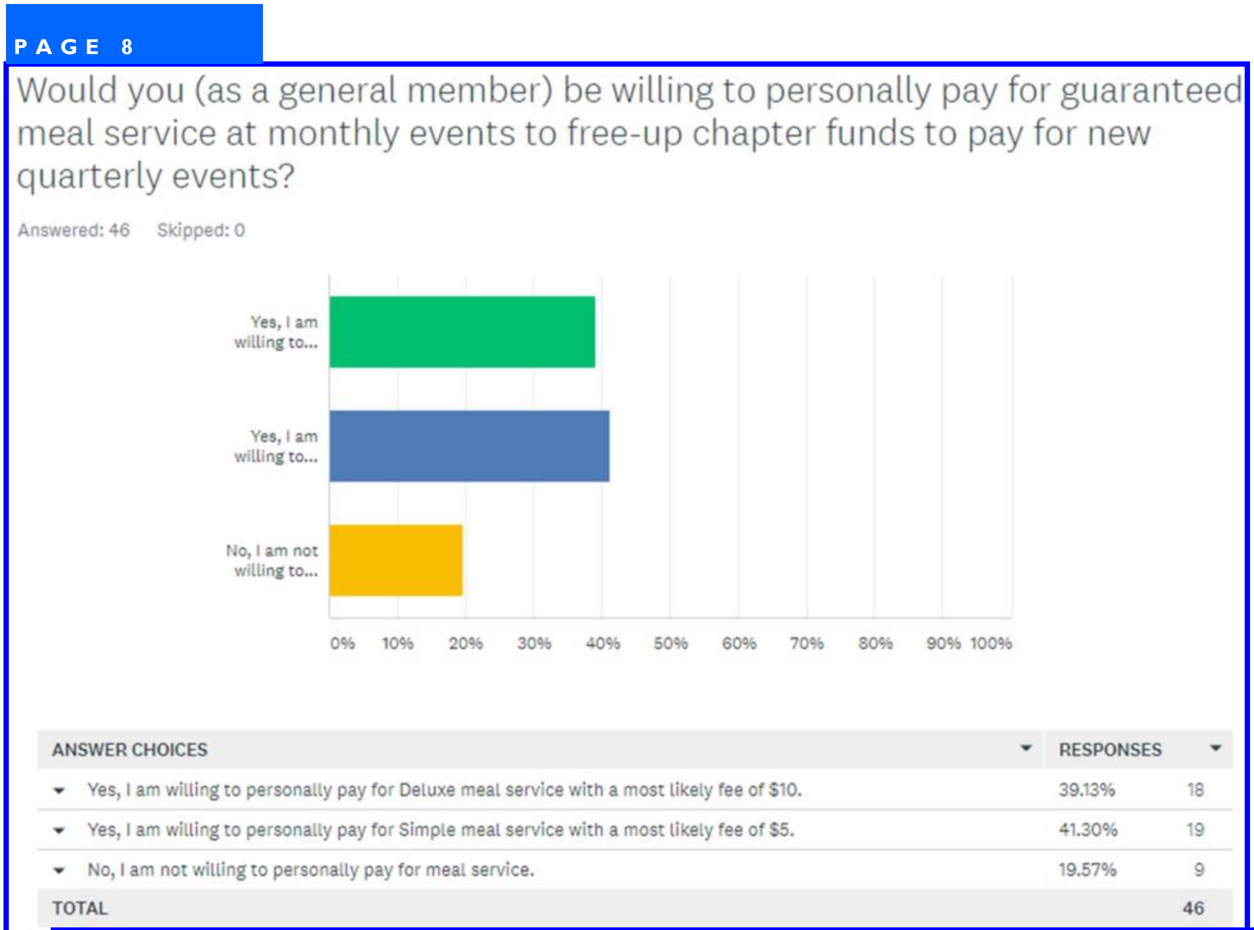
These are best read on your computer.



Would you (as a general member) be willing to see our chapter institute a financial penalty for walk-ins? Such a penalty would resemble the following format: ISSA-COS would impose a $10 fee for all non-registered walk-ins at their time of arrival.

Answered: 46 Skipped: 0

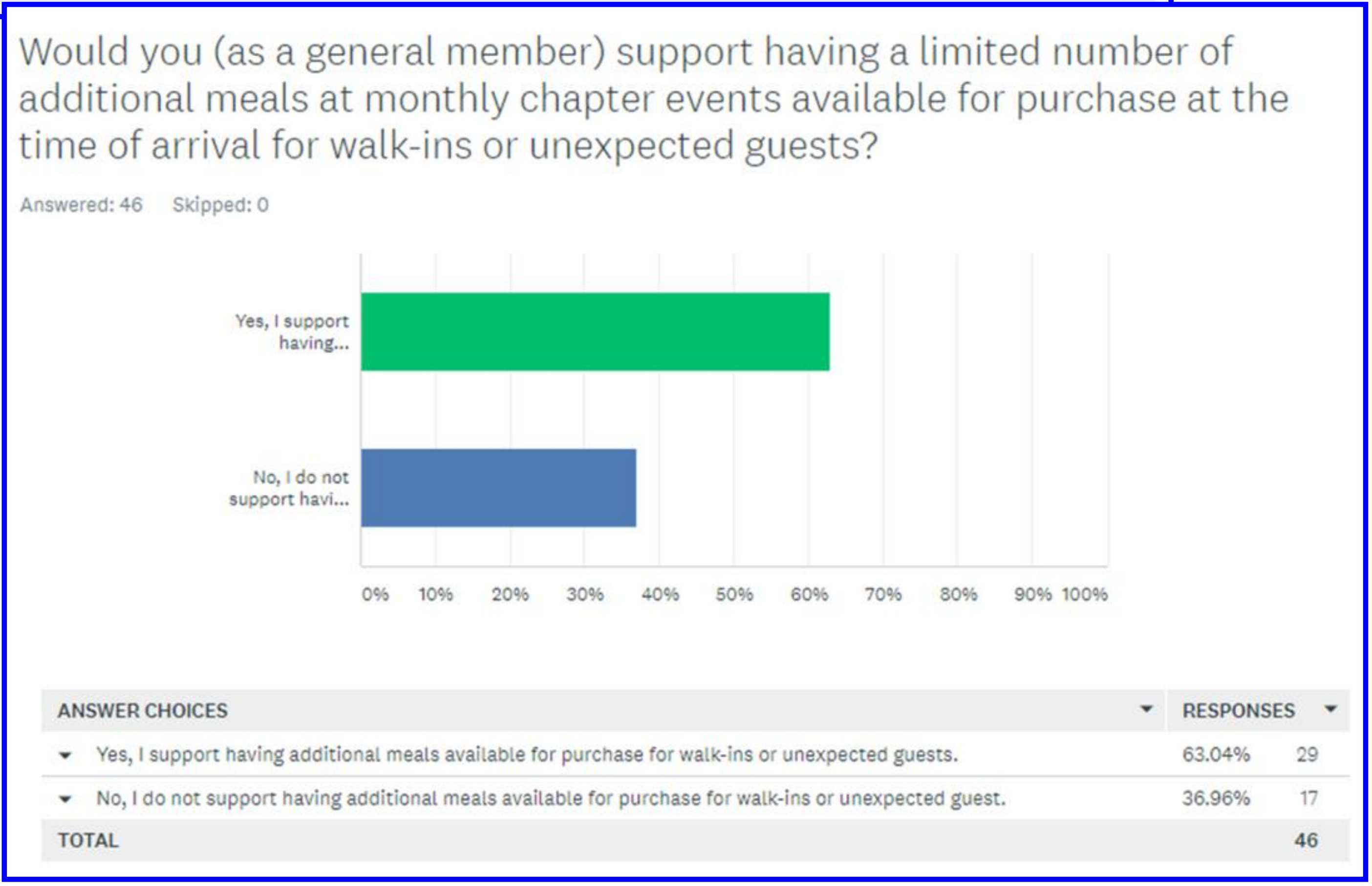
ANSWER CHOICES	RESPONSES	
Yes, I agree with instituting a penalty for walk-in attendees in the amount of $10.	69.57%	32
Yes, I agree with instituting a penalty for walk-in attendees in an amount greater than $10.	4.35%	2
Yes, I agree with instituting a penalty for walk-in attendees in an amount less than $10.	4.35%	2
No, I do not agree with instituting a penalty for walk-in attendees of any amount.	21.74%	10
TOTAL		46



Would you (as a general member) be willing to personally pay for guaranteed meal service at monthly events to free-up chapter funds to pay for new quarterly events?

Answered: 46 Skipped: 0

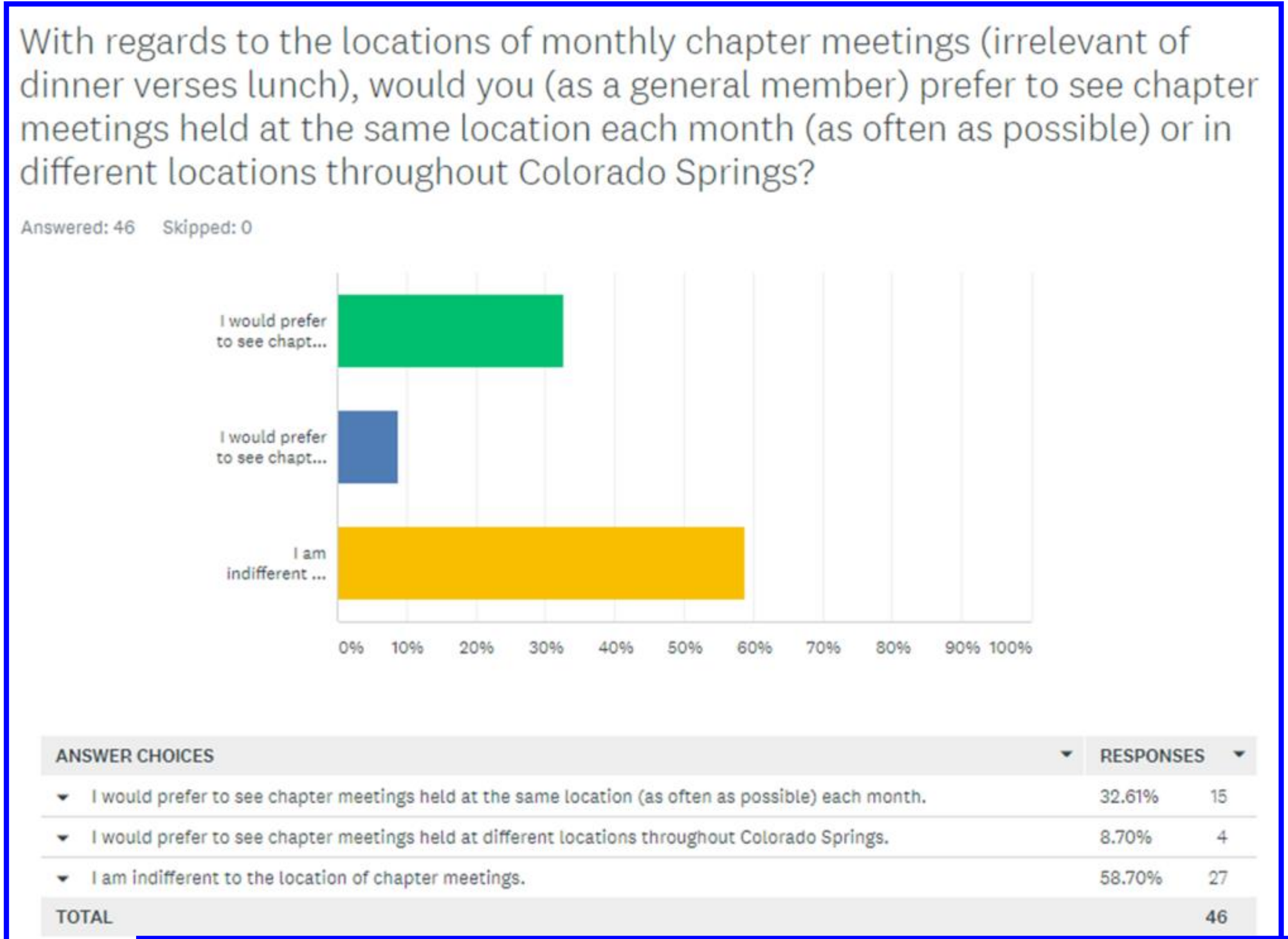
ANSWER CHOICES	RESPONSES	
Yes, I am willing to personally pay for Deluxe meal service with a most likely fee of $10.	39.13%	18
Yes, I am willing to personally pay for Simple meal service with a most likely fee of $5.	41.30%	19
No, I am not willing to personally pay for meal service.	19.57%	9
TOTAL		46



Would you (as a general member) support having a limited number of additional meals at monthly chapter events available for purchase at the time of arrival for walk-ins or unexpected guests?

Answered: 46 Skipped: 0

ANSWER CHOICES	RESPONSES	
Yes, I support having additional meals available for purchase for walk-ins or unexpected guests.	63.04%	29
No, I do not support having additional meals available for purchase for walk-ins or unexpected guest.	36.96%	17
TOTAL		46

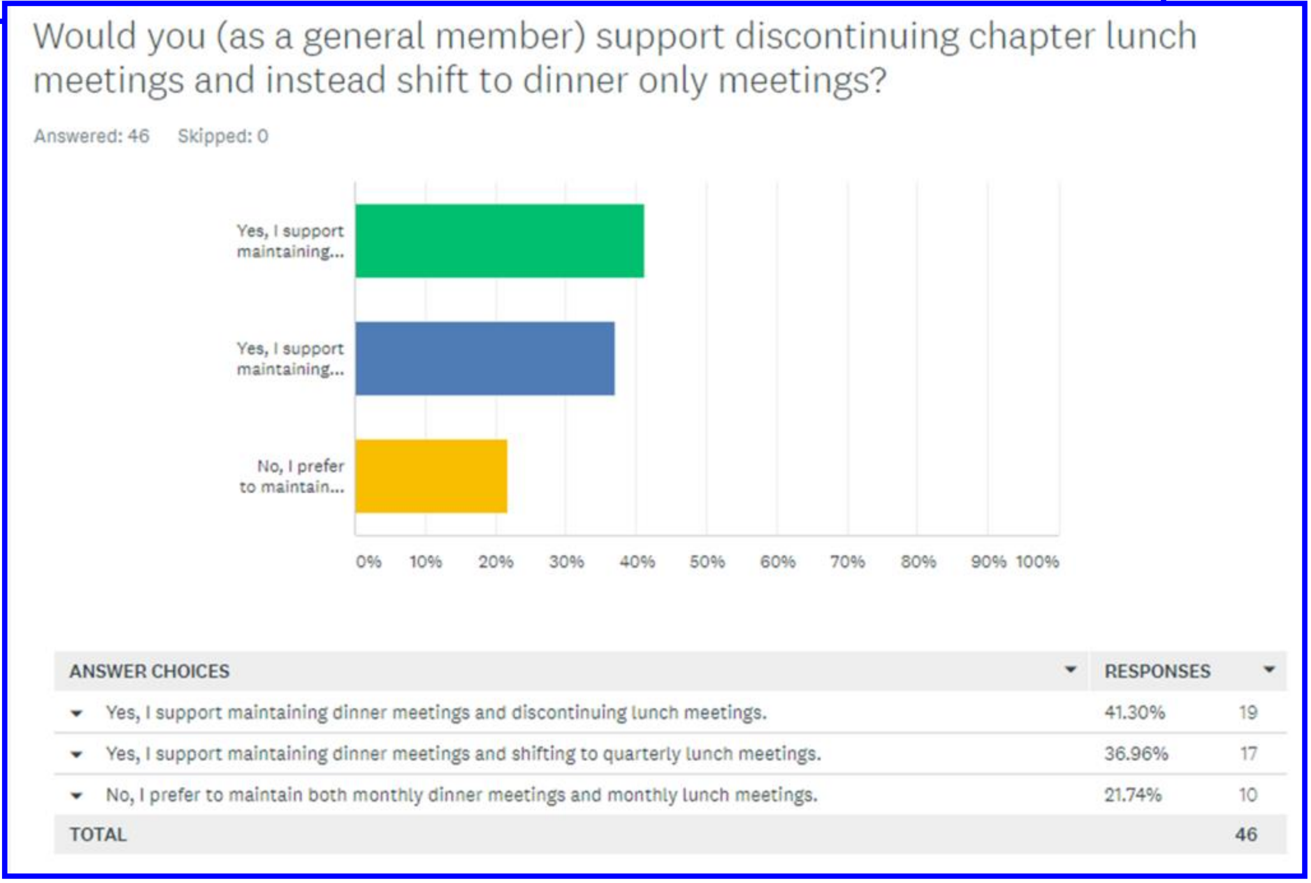


With regards to the locations of monthly chapter meetings (irrelevant of dinner verses lunch), would you (as a general member) prefer to see chapter meetings held at the same location each month (as often as possible) or in different locations throughout Colorado Springs?

Answered: 46 Skipped: 0

I would prefer to see chapt...
I would prefer to see chapt...
I am indifferent ...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

ANSWER CHOICES ▾	RESPONSES ▾	
▾ I would prefer to see chapter meetings held at the same location (as often as possible) each month.	32.61%	15
▾ I would prefer to see chapter meetings held at different locations throughout Colorado Springs.	8.70%	4
▾ I am indifferent to the location of chapter meetings.	58.70%	27
TOTAL		46

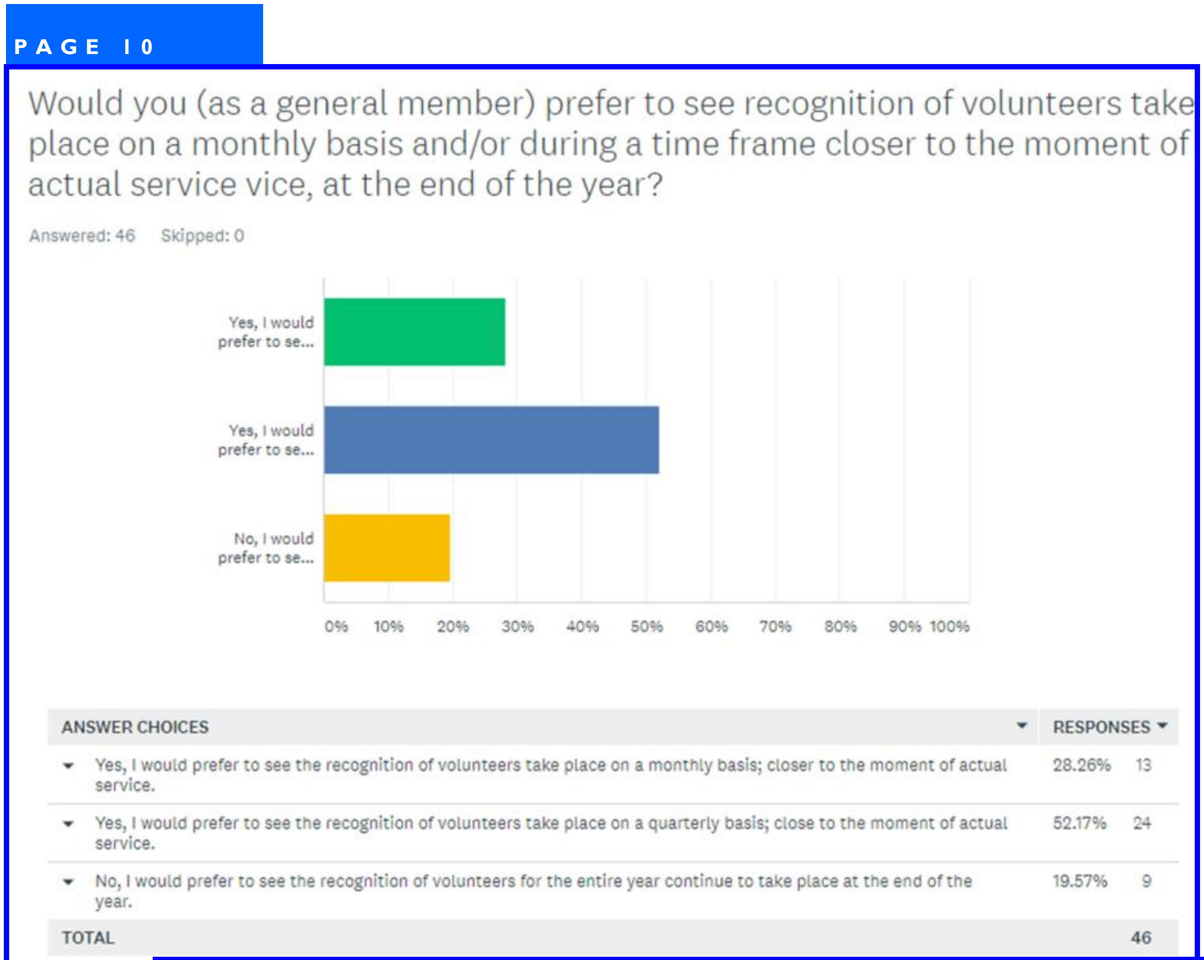


Would you (as a general member) support discontinuing chapter lunch meetings and instead shift to dinner only meetings?

Answered: 46 Skipped: 0

Yes, I support maintaining...
Yes, I support maintaining...
No, I prefer to maintain...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

ANSWER CHOICES ▾	RESPONSES ▾	
▾ Yes, I support maintaining dinner meetings and discontinuing lunch meetings.	41.30%	19
▾ Yes, I support maintaining dinner meetings and shifting to quarterly lunch meetings.	36.96%	17
▾ No, I prefer to maintain both monthly dinner meetings and monthly lunch meetings.	21.74%	10
TOTAL		46

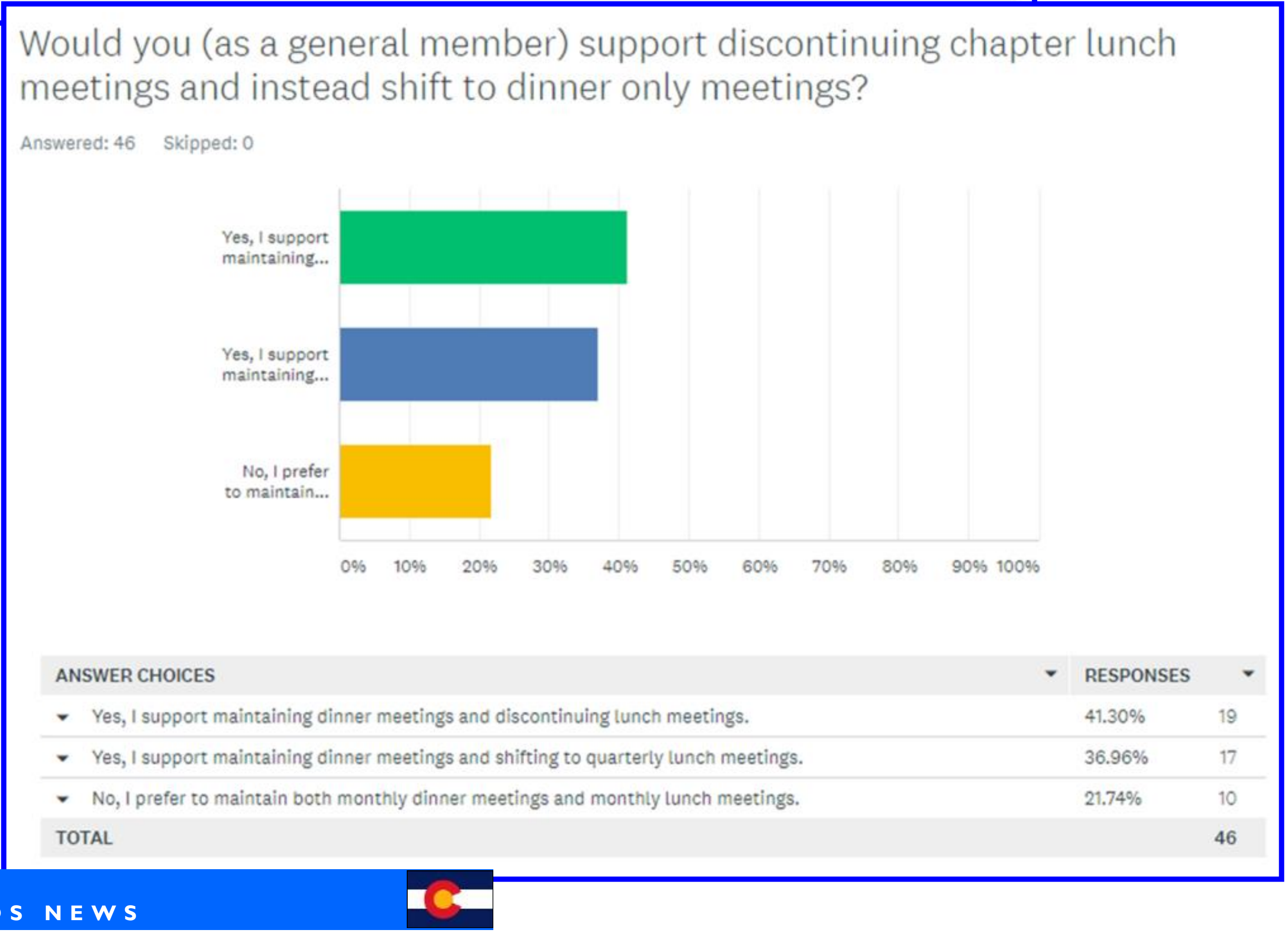


Would you (as a general member) prefer to see recognition of volunteers take place on a monthly basis and/or during a time frame closer to the moment of actual service vice, at the end of the year?

Answered: 46 Skipped: 0

Yes, I would prefer to se...
Yes, I would prefer to se...
No, I would prefer to se...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

ANSWER CHOICES	RESPONSES	
Yes, I would prefer to see the recognition of volunteers take place on a monthly basis; closer to the moment of actual service.	28.26%	13
Yes, I would prefer to see the recognition of volunteers take place on a quarterly basis; close to the moment of actual service.	52.17%	24
No, I would prefer to see the recognition of volunteers for the entire year continue to take place at the end of the year.	19.57%	9
TOTAL		46

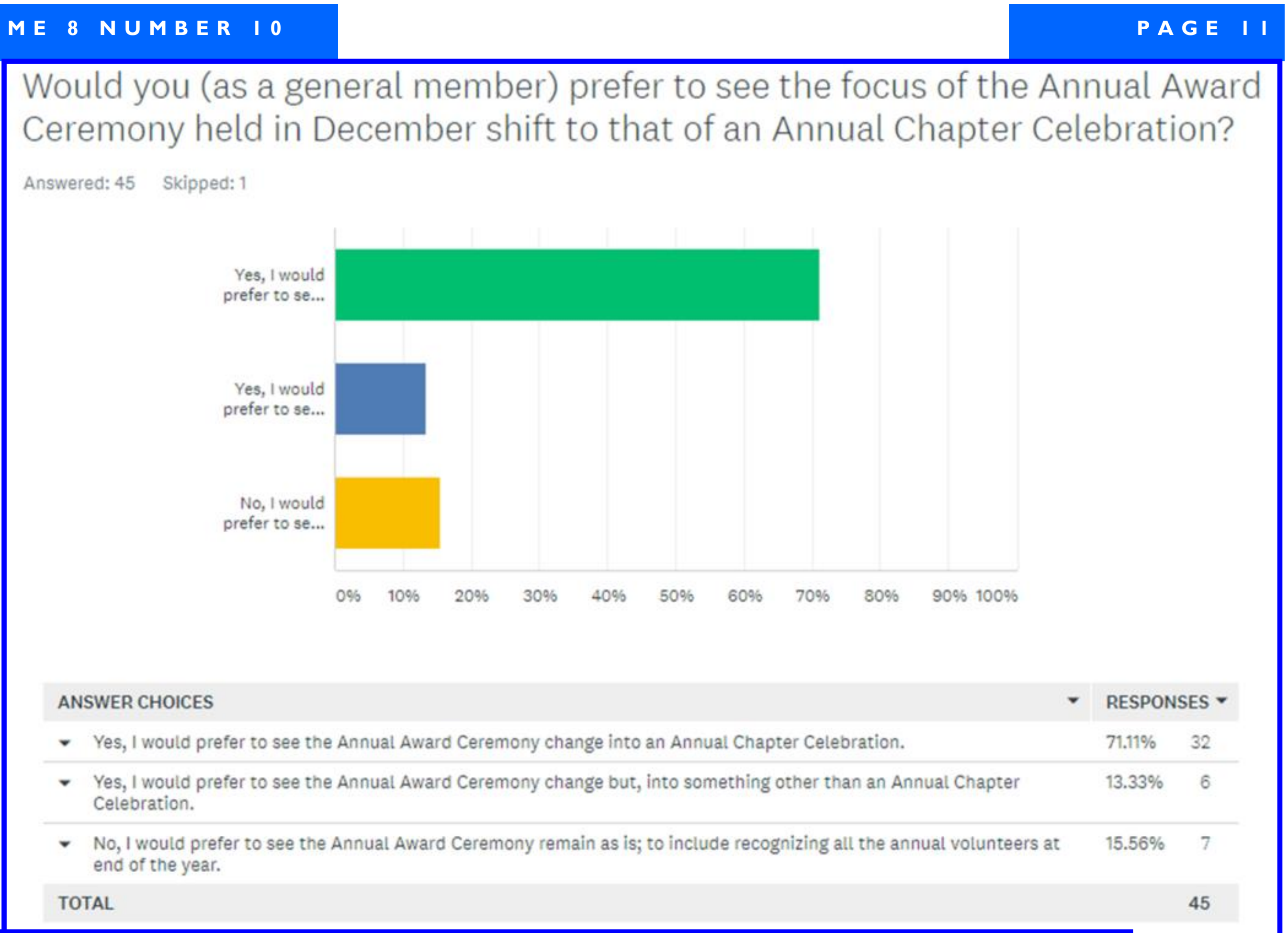


Would you (as a general member) support discontinuing chapter lunch meetings and instead shift to dinner only meetings?

Answered: 46 Skipped: 0

Yes, I support maintaining...
Yes, I support maintaining...
No, I prefer to maintain...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

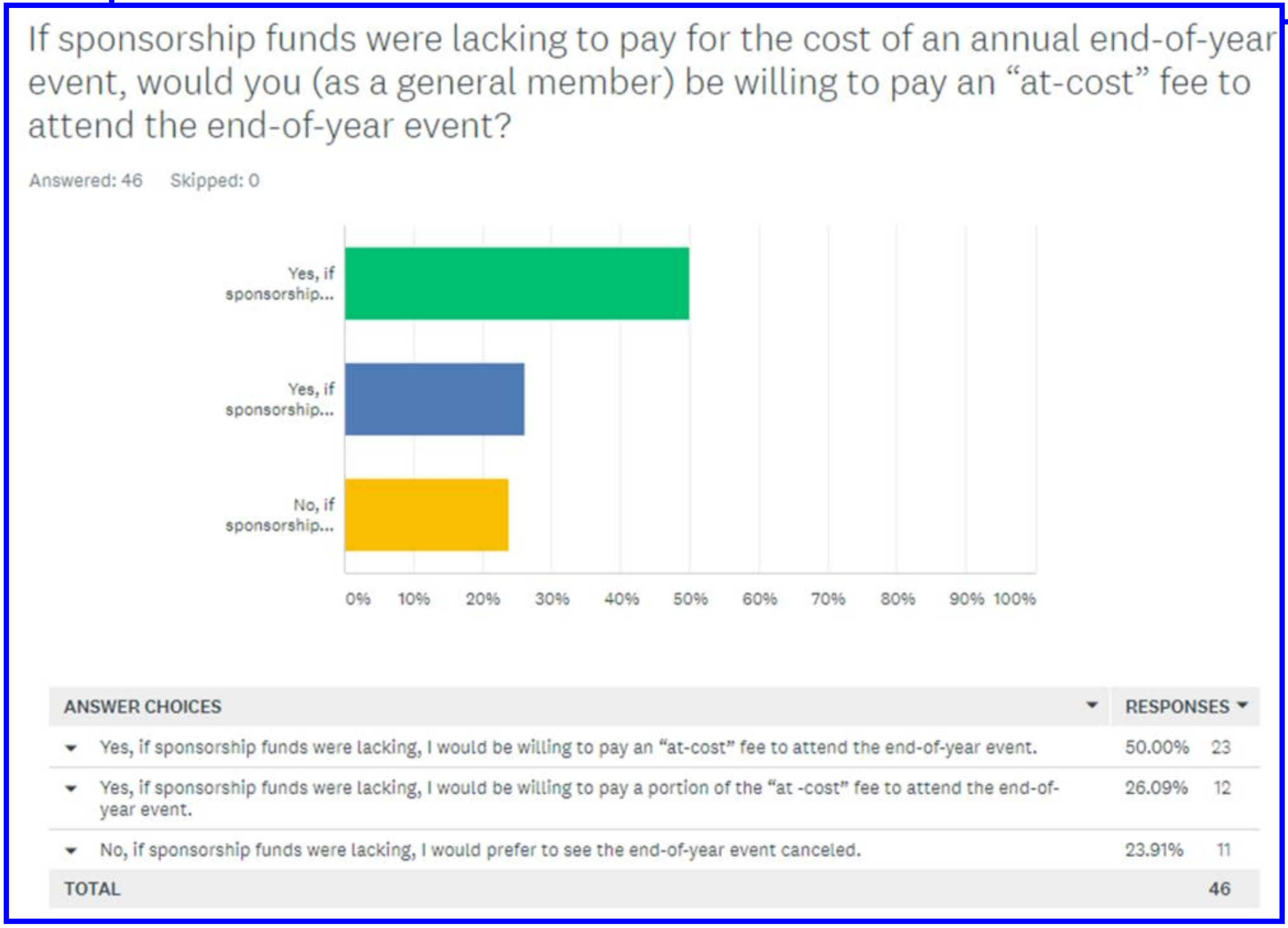
ANSWER CHOICES	RESPONSES	
Yes, I support maintaining dinner meetings and discontinuing lunch meetings.	41.30%	19
Yes, I support maintaining dinner meetings and shifting to quarterly lunch meetings.	36.96%	17
No, I prefer to maintain both monthly dinner meetings and monthly lunch meetings.	21.74%	10
TOTAL		46


Yes, I would prefer to se...
Yes, I would prefer to se...
No, I would prefer to se...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Would you (as a general member) prefer to see the focus of the Annual Award Ceremony held in December shift to that of an Annual Chapter Celebration?

Answered: 45 Skipped: 1

ANSWER CHOICES	RESPONSES	
Yes, I would prefer to see the Annual Award Ceremony change into an Annual Chapter Celebration.	71.11%	32
Yes, I would prefer to see the Annual Award Ceremony change but, into something other than an Annual Chapter Celebration.	13.33%	6
No, I would prefer to see the Annual Award Ceremony remain as is; to include recognizing all the annual volunteers at end of the year.	15.56%	7
TOTAL		45



If sponsorship funds were lacking to pay for the cost of an annual end-of-year event, would you (as a general member) be willing to pay an "at-cost" fee to attend the end-of-year event?

Answered: 46 Skipped: 0

ANSWER CHOICES	RESPONSES	
Yes, if sponsorship funds were lacking, I would be willing to pay an "at-cost" fee to attend the end-of-year event.	50.00%	23
Yes, if sponsorship funds were lacking, I would be willing to pay a portion of the "at -cost" fee to attend the end-of-year event.	26.09%	12
No, if sponsorship funds were lacking, I would prefer to see the end-of-year event canceled.	23.91%	11
TOTAL		46

What the education industry must do to protect itself from cyber attacks

By Charlie Sander, Help Net Security, August 28, 2019

Data breaches show no signs of slowing down and companies across many industry verticals fall victim to what now seems to be a regular occurrence.

Most attention around data breaches is on the commercial side, with Capital One being the recent high-profile breach, compromising the personal information of more than 100 million people. However, the education sector is proving to also be an attractive target.

This summer made it evident that K-12 school districts, higher education, and even commercial companies working with educational institutions are at risk. Notably, the state of Louisiana declared a state of emergency following an attack that disabled computers at three school districts. And it's not just a problem in Louisiana — schools nationwide are being targeted by hackers.

On August 2, the K-12 Cybersecurity Resource Center's K-12 Cyber Incident Map reported its 533rd publicly disclosed cyber incident, which means the number of data breaches against K-12 school districts in 2019 has already surpassed 2018's total. With four months still to go until the end of the year and the 2019-2020 school year beginning, school districts must take appropriate measures to protect themselves from the next attack.

Each year, more schools make the transition to the cloud and security falls further behind. The adoption of cloud technology in schools means that not only must security teams have the resources to monitor for suspicious and malicious activity from external threats, they must also simultaneously be well-equipped to monitor for potential threats from within.

The start of the school year means millions of students and staff members will return to a school's cloud environment. It also means massive amounts of data will flow into, within and out of that environment. Computers, laptops, and cloud applications like Google G Suite and Microsoft 365 are now as essential to a school supply list as notebooks, binders and pencils. Teachers and staff members use these cloud-based productivity applications as much as they do email, spreadsheets and word processing.

The fact is, schools today cannot function without these education-oriented cloud technologies and applications. At the same time, funding shortages mean that securing them is often not prioritized. But hackers are aware of this and schools should protect themselves moving forward.

Here are three ways to get the ball rolling:

1. Shift the focus to prevention, not mitigation

Most school districts have fewer than 2,500 students and don't have a staff member dedicated to handle cyber security incidents. Because of this, schools have become a target.

But their mindset should shift from "if an attack happens" to "when an attack happens."

Many schools across the U.S. have made the transition — or eventually will — to running classroom and administrative operations in the cloud. The problem, however, is that securing the cloud applications in the new cloud environment has been an afterthought. This means schools are leaving student data vulnerable to identity theft, fraud, and other emerging threats.

By shifting the focus to secure applications and data before an attack happens, rather than after, schools and other organizations in the education market will be better prepared to protect students, staff, and operations against an external attack or internal incident.

2. Minimize internal threats

The increase in adoption of cloud applications means schools must also improve their security posture to prevent an internal incident. K-12 schools that have recently transitioned to the cloud, or are still making the transition, may not realize cyber security means more than securing a network with firewalls and gateways. It also means securing the data within the cloud environment — even when an individual and device physically leaves the premises.

Verizon's 2019 Data Breach Investigations Report found that nearly 32 percent of breaches involved phishing, 34 percent involved internal actors and that errors were causal events in 21 percent of breaches. Focusing on cloud application security as much as network or endpoint security will help minimize the internal threats that could occur throughout the school year and will help prevent sensitive data from leaving a school's environment.

Read the rest here:

https://www.helpnetsecurity.com/2019/08/28/education-industry-cyber-attacks/

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.

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

Murray

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

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

Update Your Profile!

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

GAO Identifies Significant Cybersecurity Risks in US Electric Grid

By Ryan Stewart, Cyware, September 27, 2019

People around the world may be worried about nuclear tensions rising, but I think they're missing the fact that a major cyberattack could be just as damaging – and hackers are already laying the groundwork.

- The GAO determined that the electric grid faces significant cybersecurity risks and is becoming more vulnerable to cyberattacks by threat actors and criminal groups.
- The GAO has also made recommendations to the Department of Energy (DOE) and the Federal Energy Regulatory Commission (FERC).

The new report released by the Government Accountability Office (GAO) reveals that the nation's electric grid is becoming more vulnerable to cyberattacks.

What did GAO do?

The GAO reviewed the cybersecurity of the nation's electric grid, analyzed the Department of Energy (DOE) strategy for addressing the cybersecurity risks faced by the electric grid, and assessed the extent to which FERC-approved the standards to address the grid's cybersecurity risks.

What did GAO find?

The GAO determined that the electric grid faces significant cybersecurity risks and is becoming more vulnerable to cyberattacks by threat actors and criminal groups.

- The GAO identified key vulnerable components and processes used in the grid that could be exploited.
- This includes the increased use of consumer Internet of Things (IoT) devices connected to the internet, and the use of GPS to synchronize grid operations.
- The GAO also identified the potential impact of cyberattacks on the grid which includes widespread power outages in the United States.

"Although cybersecurity incidents reportedly have not resulted in power outages domestically, cyberattacks on industrial control systems have disrupted foreign electric grid operations. In addition, while recent federal assessments indicate that cyberattacks could cause widespread power outages in the United States, the scale of power outages that may result from a cyberattack is uncertain due to limitations in those assessments," the report read.

GAO's recommendations

The Government Accountability Office (GAO) has made recommendations to the Department of Energy (DOE) and the Federal Energy Regulatory Commission (FERC).

Recommendations to DOE:

- To develop a plan for implementing the federal cybersecurity strategy for the electric grid, and
- To ensure that the plan addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid.

Read the rest here:

https://cyware.com/news/gao-identifies-significant-cybersecurity-risks-in-us-electric-grid-f8e1700b

Read the report here:

https://www.gao.gov/assets/710/701079.pdf

2019 Schedule of Events

Chapter Meetings – Dinner

Tuesday, October 15, 2019

Tuesday, November 19, 2019

Chapter Meetings – Lunch

Wednesday, October 16, 2019

Wednesday, November 20, 2019

Board Meeting

TBD

Mini-Seminars

Saturday, October 19, 2019

Saturday, November 23, 2019

Special Interest Group Gatherings (see Page 13)

Thursday, December 5, 2019

Quarterly Recognition & Networking Events

Thursday, December 5, 2019

Annual Award Ceremony

Thursday, December 5, 2019

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

From the Mentorship Team

ISSA-COS Mentorship is available as an embedded feature/service which is matrixed through each SIG. This custom-tailors ISSA-COS Mentorship so that it tailor-fits each career lifecycle stage and special interest. ISSA Mentors and Proteges aren't enrolled into a mentorship program; rather, the process is that of an intake in which a need is assessed with the goal of the need being met. The need is taken in and evaluated and an action plan is created to meet the need. (As an additional need arises, an additional intake is created.)

ISSA Mentorship is an exchange in which both parties are protected and respected. Healthy boundaries are maintained and proprietary knowledge is protected. ISSA Mentorship is designed to be a win-win situation in which both parties are enriched.

ISSA Mentorship is goal/need-driven. The ISSA-COS Mentorship Intake Form serves as a guide regarding the length of the mentorship session as the goal/need of the mentor or protege will determine parameters. The carefully-crafted intake form provides ISSA-COS leadership with metrics so that ISSA Mentorship is treated as a service with KPIs (Key Performance Indicators) and next step suggestions. If ISSA-COS Mentorship can *measurably* boost the careers of its membership, ISSA will, in turn, be boosted as we become known for building each other.

Mentorship Intake Form

email completed form to: mentorship@issa-cos.org

Colorado Springs Chapter
ISSA
Information Systems Security Association

I seek to:

- ❏ mentor
- ❏ protégé
- ❏ peer-to-peer

I aim to meet:

- ❏ in person
- ❏ by phone
- ❏ via email
- ❏ via Skype

What drives you to invest in mentorship now? Please state two goals:_______

____

____

____

____

____

Name:_____________

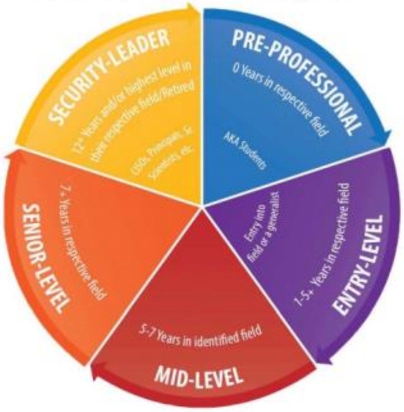
Phone:_____________

Email:

____

____

Checkmark your current status in the ISSA Cyber Security Career Lifecycle:


PRE-PROFESSIONAL
0 Years in respective field
AKA Students
ENTRY-LEVEL
1-5+ Years in respective field
Entry into field or a generalist
MID-LEVEL
5-7 Years in identified field
SENIOR-LEVEL
7+ Years in respective field
SECURITY-LEADER
12+ Years and/or highest level in their respective field/Retired
CISOs, Principals, Sr Scientists, etc.

Are you on LinkedIn? Y / N

Are you on Skype? Y / N

Have you visited the ISSA-COS website? Y / N

Which ISSA committees or special interest groups align with your interests?

- ❏ Speakers Bureau
- ❏ Friends of Authors
- ❏ Women in Security
- ❏ Healthcare in Security
- ❏ Finance in Security
- ❏ Retail in Security
- ❏ DoD in Security
- ❏ Executives in Security
- ❏ Young Professionals in Security
- ❏ certification prep
- ❏ continuing education
- ❏ other: ___________

My mentorship goals align most closely with:

- ❏ career advice
- ❏ building an alliance
- ❏ seeking opportunity
- ❏ technical training
- ❏ practice leadership
- ❏ practice speaking
- ❏ practice authoring for publications
- ❏ solving a specific technical challenge
- ❏ finding my place in our ISSA chapter
- ❏ other ___________

MENTOR USE ONLY

Feedback / Recommendations

Time invested:____ mins / hrs

Were goals met? Y / N

Is additional mentorship requested at this time? Y / N

Additional notes:

OFFICE USE ONLY

Follow-up Plan

- ❏ *time recorded*
- ❏ *goals recorded*
- ❏ *resources provided* _______________
- ❏ *referred to SIG:* ________________

Next steps:

New encryption method called ‘Splintering’ makes password hacking 14 million percent more challenging

By Cyware, ZD Net, September 9, 2019

What’s the matter?

Researchers at Tide have developed a new technique dubbed ‘Splintering’ to protect usernames and passwords. They claim that Splintering is 14 million percent more difficult to hack when compared to other techniques.

“This technique makes it tremendously more difficult to reconstruct one complete password, let alone all the passwords, using either reverse engineering or common brute force attack methods,” researchers said. Tide is a non-profit foundation focusing on building data privacy focused technologies.

How does this technique work?

Researchers at Tide have implemented the new splintering technique in Tide Protocol. This technique takes encrypted passwords within an authentication system, breaks them up into multiple splinters or fragments, and stores them on a decentralized distributed network from where they can be reassembled when required.

- The number of splinters that each encrypted password is broken up depends upon the desired cryptographic strength and the organization’s requirements.
- The minimum number of splinters is 20 nodes.
- Each node is assigned to a splinter and can be assembled when requested.
- Only the node assigned to a splinter can decrypt and assemble the splinter.

Key findings

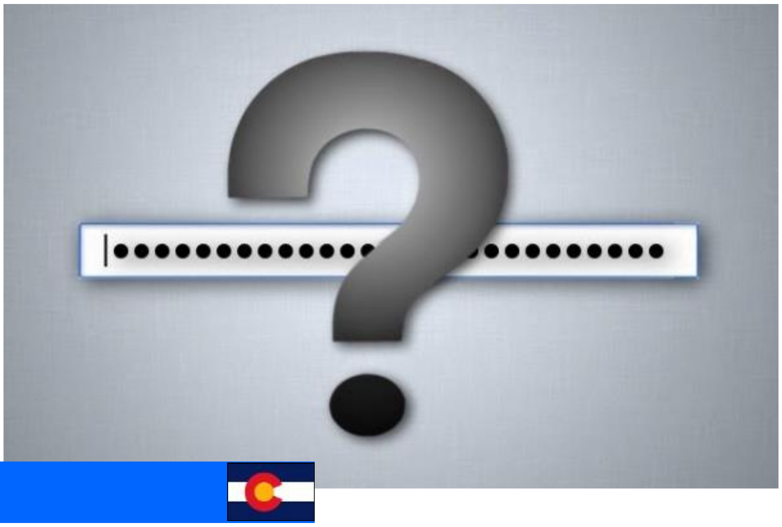
Tide researchers tested the splintering technology against 60 million LinkedIn passwords that were previously breached.

- The test revealed that splintering reduced the odds of a successful dictionary attack from 100% to 0.00072%, which is a 14 million percent improvement.
- Splintering allows up to 30% redundancy, which means that the splintered passwords can be fully reassembled even if up to 6 nodes storing the splinters were to become unavailable for some reason.
- End-to-end latency results showed that the splintering process takes between 1,500 milliseconds to 4,000 milliseconds with a full complement of nodes across Microsoft Azure, Google, and Amazon networks.

Tide has introduced an intentional built-in 300-millisecond delay for each authentication request to mitigate brute-force and denial-of-service attacks on the network. Despite this, the latency result proved that the latencies associated with the splintering process are better than existing commonly used authentication methods.

Read the rest here:

https://www.zdnet.com/article/ameo-concerned-about-nation-state-attacks-on-power-grids/



DOD Will Require Vendor Cybersecurity Certifications By This Time Next Year

By Aaron Boyd, NextGov, September 6, 2018

The government has stringent processes for verifying the IT products and services it uses comply with relevant cybersecurity standards, such as authorities to operate for cloud services and supply chain regulations for hardware products. But those standards and processes don't cover the vendors.

For the Defense Department, this is a critical issue, as doing business with industry requires the department to share sensitive information, even at the earliest steps of the process.

The department has been kicking around the idea of creating a certification standard for defense industrial base companies to ensure vendors' cybersecurity posture was adequate to handle controlled and classified information. That became an official effort in March, and Wednesday the department released the first draft Cybersecurity Maturity Model Certification, or CMMC, outline for public comment.

At the top level, the framework covers 18 domains, described as "key sets of capabilities for cybersecurity" in a slide deck distributed by the Office of the Assistant Secretary of Defense for Acquisition. These domains include areas like access control, governance, incident response, risk assessment and the like.

Each domain is then assessed based on practices—the "activities performed at each level"—and processes—the level of maturity for each practice within the organization. By splitting this into two buckets, vendors can show that they have institutionalized the "processes," even if they don't get perfect marks on any given "practice" at the time of assessment.

Both practices and processes are assessed across five levels, from basic to advanced and optimized, respectively. The result is a five-tier system, each pegged to a certain level of cybersecurity assurance.

"For a given CMMC level, the associated practices and processes, when implemented, will reduce risk against a specific set of cyber threats," the slide deck reads.

The tiered system is intended to make it easier for the department to streamline certification requirements, as well as to allow small businesses and others to tailor their efforts—read: costs—to their specific needs.

At the lowest level, practices include things like abiding by Federal Acquisition Regulation requirements and having basic antivirus installed on systems. At the highest tier—level five—practices are beefed up to include customized cybersecurity software, employing 24/7 security operations centers and automated incident response.

Once the maturity levels are established, the department plans to work with third-party assessment organizations to "conduct audits and inform risk," similar in structure to the civilian Federal Risk and Authorization Management Program, or FedRAMP, which uses third-party contractors, dubbed 3PAOs, to verify the cybersecurity of cloud products.

The model is currently in its fourth draft, which the department released for public comment Wednesday. The department expects to be on the sixth draft by November and plans to issue the first release of the final version in January.

At this time, Defense officials expect the scope of the model to go down in size, rather than expand, as officials garner feedback, eliminate redundancies and down-select to the most important requirements.

The contracting community will have some additional time to absorb the final version—but not much. Defense offices will be expected to include certification requirements in requests for information by June 2020 and in solicitations by fall of next year.

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/09/dod-will-require-vendor-cybersecurity-certifications-time-next-year/159702/

2019 PEAK CYBER

GDIT Delivering Cyber to Agencies at Scale
DEFENSE
FEDERAL CIVILIAN
6391+ Cyber Certifications
30+ CUSTOMER AGENCIES
>3K Cyber Professionals
10+ SOCS
Supporting largest Cyber Operations in the federal government (SOCS)
GDIT
EXIT

ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce

Many additional photographs are available on the [ISSA-COS.ORG]() website.

Matthew Toth
Splunk

PEAK CYBER
WELCOME TO THE 9TH
PEAK CYBER SYMP
EXIT
DOUBLETREE

WWW.ISSA-COS.ORG

Chapter Officers:

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: **Vacant**

- 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: Dennis Kater

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*

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

Significant Interest Group Leads:

Chair: Anna Parrish
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

'Security' Cameras Are Dry Powder for Hackers. Here's Why

By Robert Hackett, Fortune, September 19, 2019

Researchers have long bemoaned the insecurity of certain "security" cameras. Ostensibly installed to deter and thwart intruders, many actually can be transformed into an arsenal that hackers use for Web warfare.

The latest cause for concern: A vulnerability that enables hackers to summon a firehose of network traffic from hundreds of thousands of such devices for "distributed denial of service" attacks, also known as "DDoS" attacks, that aim to knock targets offline—sometimes just for kicks and giggles, other times until a victim pays ransom. In a report published Wednesday, security researchers at "cloud" network firm Akamai called attention to the recently identified flavor of attack, warning that instances of it are likely to worsen, in coming weeks, in terms of severity and frequency.

Read the rest here:

https://fortune.com/2019/09/19/security-cameras-are-dry-powder-for-hackers-heres-why/

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