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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 8

AUGUST 2019

Lots for August

A Note From Our President

By Mr. Ernest Campos

ISSA-COS Members,

Welcome to August and the peak of summer! Speaking of "peak," have you registered for the **2019 Peak Cyber Symposium** yet? We are less than 30-days way from our 9th year of hosting this nationally attended event. This year includes a Capture the Flag (CTF) challenge sponsored and facilitated by SPLUNK, a symposium kickoff dinner with a special guest speaker, four (4) opening/closing keynote speakers, multiple panel discussions, fifteen (15) individual training breakout sessions, eight (8) individual Special Interest Group (SIG) breakout sessions, an exhibit hall with forty (40) vendor booths, and nearly $10,000 in raffle prizes!! I don't know how we could possibly fit anything more into this 3-day event! If you haven't registered yet, please do so now. Right now. Like, stop reading this message and go register at www.fbcinc.com/peakcyber. Now. Go. …Thanks! But, please come back when you are done registering to finish reading this very important letter.

Looking back at July, our chapter enjoyed great presentations from **Mr. Rob Carson** (Chapter Dinner & Lunch meetings) and **Ms. Gretchen Bliss** (Mini seminar). Both speakers provided outstanding messages for our members with lots of positive feedback. Also, in July, our chapter was honored to be asked by the World Affairs Council and U.S. Department of State to host another round table panel discussion for a group of visiting international delegates. This event featured 18 delegates from sixteen (16) European countries. Our chapter was proud to assemble a panel of Global and Government Cybersecurity professionals from our local Colorado Springs area who not only represented our chapter in fine fashion but, also fielded a barrage of very challenging questions for 2-hours straight. In the end, we demonstrated our savvy and depth of knowledge related to Cybersecurity governance, policy, and operational programmatic processes. Our chapter extends a special "Thank You" to **Steven Mulig, Darla Lindt, Eric Bailey, and Julia Costin** (accompanied by **Dr. Gurvirender Tejay)** for stepping up to represent ISSA-COS with professionalism, pride, and expertise.

Shifting gears, the rest of this message is dedicated to some **sobering** chapter business. Soon, I will release a survey to all general members designed to let each of you

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.

'I kept my multimillion dollar business secret'

By Joe Tidy, BBC News, July 22, 2019

A lot of entrepreneurs have "a moment". A moment that makes them realise they're on to something.

For Marcin Kleczynski it came while he was discreetly working on his antivirus software business from his student digs.

His start-up company Malwarebytes was less than a year old back in late 2008, but already gaining a good reputation in the cyber security world.

Marcin, then only 18, was just about managing to juggle running his start-up with participating in student life at the University of Illinois when he hit a snag.

"I was having some real trouble analysing the latest computer virus, when all of a sudden I get a white page on my screen that says 'you've been banned from the school network due to malicious activity on your desktop'," he says.

"They'd obviously detected that I had a virus on my computer, but didn't realise it was deliberate. So I call the university IT helpline, and they send a kid, no older than me. He sits down at my computer and looks at it and says 'boy you've really screwed this thing up'.

"Then, right in front of me, he logs onto my website and downloads Malwarebytes.

"I didn't say anything, I stood behind him and watched him fix my computer with my software to get me back online. He left never knowing who I was, but to this day I love that moment."

> *“You've heard my story, I started the company when I was living with my parents.”*

By the time Marcin graduated with a degree in computer science in 2012, he had quietly grown Malwarebytes into a business earning a few million dollars a year. All without any of his lecturers having any idea what was taking up his time, and pushing his grades down.

Today the company has an annual turnover of more than $126m, and millions of customers around the world.

Born in Poland in 1989, Marcin moved to the US with his family when he was three, settling in Chicago.

As a gaming-obsessed teenager, he'd accidentally got a virus when he was 14, and learned everything he needed to know about computer bugs from internet forums and a "For Dummies" book.

Formally launching Malwarebytes in January 2008 when he was just 18, it grew quickly, and he decided that starting university in September of that year would just slow him down. His mother had other thoughts.

"The business was becoming real, and so I went sheepishly to my mum and said 'I don't think I'm going to go to school'," says Marcin. "Fifteen seconds later we were packing my stuff and I was going to school."

What made Mrs Kleczynski initially more alarmed was that her teenage son had launched the business with a man in his 30s called Bruce Harrison. Marcin and Bruce had been writing software together for more than a year, after they first started talking on anti-virus forums.

"Here's this 17-year-old kid... he's this 35-year-old man. Imagine telling your mum?..." says Marcin.

Marcin and Bruce hadn't actually met in person at the time. Bruce was a computer repairman in Massachusetts, and Marcin was at home in Chicago. They didn't in fact see each other in the flesh until Malwarebytes was more than 12 months old.

"We didn't meet until we made our first million about a year after we launched the product," says Marcin. "Even that was kind of anti-climatic. It was just, 'Hey, Bruce!' - We had a handshake and moved on."

Today Bruce, who is head of research, still lives and works on the US east coast, while Marcin is based in the head office in Silicon Valley. The company now has more than 750 employees, and overseas offices in the Republic of Ireland, Singapore and Estonia. Since 2014 it has secured $80m of investment funding.

Read the rest here:

https://www.bbc.com/news/business-49015609

Membership Corner

Membership Update

First, 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.

New Members July
Rebecca Botvinik
Ike Mast
Justin Whitehead
Jon E. Martin
Mitch Willoughby
Wendy Bricker

We're working hard on the upcoming Peak Cyber Symposium, 3—5 September at the DoubleTree by Hilton, Colorado Springs. Attendance is free for all ISSA-COS, ISSA-Denver, and ISSA-Northern Colorado as well as anyone with a .mil, .gov, or .edu email address. This is an exceptional chance to showcase our chapter so let all your colleagues know about it. It's also a great opportunity to volunteer to support the chapter. If you're interested in volunteering, please let any board member know. You don't have to commit a lot of time—an hour or two helps a lot. The more volunteers we have, the less time any one individual is needed. Please take a minute to register at the Federal Business Council (FBC) website at https://www.fbcinc.com/e/PeakCyber/attendeereg.aspx . Early registration gives us a big leg up when trying to recruit sponsors for the event and the chapter.

The Peak Cyber Symposium is also one of our most effective membership recruiting tools that we have. As our membership has dropped a bit to ~444 members as of the end of July, it is critical that we leverage the Symposium to show potential members the benefits of membership. Please take a minute to talk to your co-workers about attending.

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

If you want to learn more about the Cybersecurity Maturity Model Certification go here:

https://www.acq.osd.mil/cmmc/faq.html

(Continued from page 1)

guide and shape our transformation from an organization into a community institution. Evidence supporting the timeliness of this transformation includes invitations our chapter has received to participate in high-profile local and national events, invitations received from peer community organizations to merge annual cornerstone events, and invitations received from higher-caliber organizations to enter into significant partnership agreements.

A Note From Our President

To succeed in this institutional transformation, our chapter will need to continue our efforts to streamline and standardize our operational business rhythm. This includes focusing our attention on where and how we spend our resources; to include time, efforts, and volunteer manpower such that it yields the greatest return on their individual investments.

As such, the survey I will soon release will include the following questions focused on how we can become better stewards of our chapter resources. It has been a long-held principle that our chapter exists solely to promote and present the best interest and opportunities for and to our general members. It is along these lines that I will present the following questions for everyone's consideration.

Optional Meal Fees:

For multiple years now, our chapter has been plagued by a consist problem: the issue of dealing with no-show registrants, late-registrants, and walk-ins at all our regularly scheduled events. The privilege of attending our events for free is an awesome benefit that all of us enjoy but, unfortunately, too many of us abuse. Coupled with the desire to provide free food/meals at our events, this plague has become a noticeable problem that has cost our chapter thousands of dollars over the last few years.

For those who aren't aware, let me breakdown the situation. The only "real" costs associate with our regularly scheduled events includes catering and reproduction (printing). Thanks to our annual membership with the Colorado Springs Chamber and Economic Development Corporation (EDC), we receive an incredibly generous discount on printing cost to the tune of only $0.03 per photocopy. Thus, printing fees are not an issue. The real challenge is associated with catering and that is where I will focus this conversation.

Our chapter uses our online registration system to gauge how many meals we need to order for each type of event. When 60 people register to attend an event, we order 60 meals at a cost of $10 per meal. But, when only 40-50 people arrive, we sustain a loss of 10-20 meals or $100-$200. Each month, we host a dinner chapter meeting, a lunch chapter meeting, and breakfast mini seminar. On average, over the last 2-years, our chapter has lost approximately $100 - $300 per month in catering costs due to no-show registrants. Multiplied by the 8-months/year that we host these three types of meetings, the annual loss ranges between $800 (low side) to $2,400 (high side). This represents an actual loss of chapter funds that could otherwise be used to provide additional chapter events. To confront this situation, I am presenting to our chapter the following additional survey questions:

1. Would you (as a general member) be willing to personally pay between $10 (most likely cost) and $15 (least likely cost), when required, for guaranteed meal service at regularly scheduled chapter events (i.e., chapter meetings, mini seminars, SIG gatherings, and networking events)? Such meal service would include a main entree, two sides, dessert, beverage, and meal service accessories (i.e., plates, plastic ware, napkins, etc.). (Yes or No)
2. Would you (as a general member) be willing to see our chapter invoke a financial penalty for late registrants? Such a penalty would resemble the following format: ISSA-COS would institute a $10 penalty for late registrants. Effectively, general members would be provided a declared timeframe to register for events at no-cost (free). Beyond this timeframe, late-registrants would pay a $10 fee to register for events. (Yes or No)
3. Would you (as a general member) be willing to see our chapter invoke financial penalties for walk-ins? Such a penalty would resemble the following format: ISSA-COS would institute a $10 fee for all non-registered walk-ins at their time of arrival. Walk-in fees would be collected in cash or via credit card. (Yes or No)
4. Would you (as a general member), support having ISSA-COS provision a nominal number of meals (5 – 10 meals per event) available for purchase by late registrants and/or walk-ins? Such meal fees would be collected at the time of arrival and would be paid in cash or via credit card. (Yes or No)
5. Would you (as a general member), support having chapter funds previously lost on no-show catering expenses, instead utilized to fund quarterly networking events starting in the 2020 calendar year? (Yes or No)

Chapter Lunch Meetings:

For multiple years now, our chapter has scheduled both dinner and lunch chapter meetings; effectively, doubling the effort required to host a monthly chapter meeting. Over the last 12-months, registered attendees compared to actual attendees have averaged 50-60%. By the numbers, this equates to 25-30 (actual attendees) out of 40-45 (registered attendees). Yet, the effort required to host the event is 100% regardless of 25 or 40 attendees. Also, worth noting, is the fact that our sponsors and guest speakers anticipate a specific number of attendees to justify their financial sponsorship to our chapter. When our chapter fails

(Continued on page 5)

(Continued from page 4)

to deliver on attendance, our image suffers as does our likelihood for a repeat sponsorship. For this reason, I am also adding the following survey question to the list:

6. Would you (as a general member) support having dinner only chapter meetings? Such a decision would theoretically increase attendance at chapter dinner meetings. Increased attendance at dinner events would effectively increase the attraction of prospective sponsors and guest speakers. Thus, for less effort (one meeting verses two), our chapter would experience a greater return on attendance and prospective sponsors. (Yes or No)

In a recent reflection of my performance, I was remiss in my ability to institute Quarterly Recognition and Networking events. The principle reason these events where not instituted this year was due to a lack of funding. Although sponsorship opportunities are always sought-out and welcomed, their inherent variability prevents us from being able to rely upon them for funding of standard events. Thus, if we are to successfully internalize these events as a priority part of our regularly scheduled events, we will need to establish a way to fund these events detached of sponsorships. Thus, the reason for some of the previously presented survey questions which can be summarized as follows: would you rather have free food or free access to quality networking events that also qualify for CPE/CPU credits?

With that, I leave you to reflect on your potential responses. The survey will be released within the month of August and members will have throughout the month of September to respond. Your responses will help shape the agenda for our chapter in the year 2020. Thank you in advance for your participation. And thank you for all you do to help make our chapter the best chapter in all of ISSA!

Sincerely,

Ernest

Breakfast with ISSA-COS

ISSA-COS will arrange for Oliver's Deli to come sell breakfast at your office!

Patrons will receive a **15% discount** on all food items… *compliments of ISSA-COS!*

An ISSA-COS representative will be on hand to provide membership and sponsorship information.

Nominate your company and

YOU EAT FREE!

OLiVER'S DeLi

Since 1983

LOVE LOCAL FOOD

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/

Update Your Profile!

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

Call for Articles: "Best of ISSA-COS" 2019

- Network and Infrastructure Security
- Web Security
- Endpoint Security
- Application Security
- Managed Security Service Providers
- Data Security
- Mobile Security
- Risk and Compliance
- Identity and Access Management
- Security Operations and Incident Response
- Threat Intelligence
- IoT
- Messaging Security
- Digital Rights Management
- Security Consulting
- Blockchain
- Fraud and Transaction Security
- Cloud Security

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.

Congress Passes Two Small Business Administration Cybersecurity Threat Bills

By Brett Shaw, ProofPoint, July 29, 2019

On July 15, 2019, the House passed two bills aimed at raising the awareness of cybersecurity threats to small business owners and employees.

H.R. 2331 SBA Cyber Awareness Act requires the Small Business Administration (SBA) to notify each small business within 30 days after every cybersecurity risk and incident.

Additionally, H.R. 1649 Small Business Development Center Cyber Training Act of 2019 requires the SBA to establish a cyber counseling certification program to certify 10% of SBA employees at each of the approximately 900 Small Business Development Centers to provide cyber planning assistance to small businesses. It requires these SBA employees to advise small businesses on how to develop a comprehensive cybersecurity strategy.

As reported in The Hill, “Cybersecurity is one of the biggest threats to our economy and small businesses,” noted H.R. 2331’s primary sponsor, Rep. Jason Crow (D-Colo.), in April when introducing the bill to the House. “Our small businesses are the backbone of our economy but are increasingly the target of cyber attacks and theft of small business data and intellectual property.”

These bills aim to raise the awareness of cybersecurity risks among SMBs (small and medium-sized businesses) and to help them formulate a cybersecurity strategy. Proofpoint Essentials and Proofpoint Security Awareness Training should be the cornerstones of an SMB’s cybersecurity strategy because they address the number one cybersecurity threat vector (email) and the number one risk that attackers rely on to execute attacks (employee susceptibility to social engineering attacks).

Proofpoint Essentials gives SMBs complete protection and detailed insight into threats targeting their people. Each month, Proofpoint Essentials blocks an average of 130 advanced email threats per SMB, including targeted phishing and malicious attachments.[1]

Additionally, Proofpoint Security Awareness Training is a Gartner Magic Quadrant leading solution for employee cybersecurity awareness, with phish simulation, training modules, email reporting and remediation.

Read the rest here:
https://www.proofpoint.com/us/corporate-blog/post/congress-passes-two-small-business-administration-cybersecurity-threat-bills

Volunteer Opportunities

Board Positions	Key Personnel	Volunteer Corps
Deputy Recorder/Historian **Deputy Treasurer** **Deputy VP of Training** **Member-at-Large**	**SIG Committee Chair** **Recognition Committee Chair** **SIG Leaders:** • ***Finance*** • ***Retail*** • ***Educators*** • ***Executives***	**Increase community awareness of our chapter** **Expand community involvement for our members** **Attend industry relevant events throughout Colorado** **Earn additional CPE/CPU credits** **Increase network**

Millions “Gambling with Personal Data” by Accessing Fake WIFI Hotspots, Poll Suggests

By Rob Knight, Independent, July 29, 2019

Millions of people are gambling with their personal data by blindly accessing fake wifi hotspots, according to a poll.

One in five have taken “significant risks” by failing to check if public wifi connections are legitimate – instead using hotspots which are free, seem to be credible and offer fast speeds.

Users could be connecting to misleading hotspots, which can appear to be reputable but allow cybercriminals to eavesdrop on users and steal usernames, passwords and bank details.

These wifi connections, which often have innocuous sounding names such as “airport wifi” or “hotel wifi”, can also redirect victims to malicious malware sites and phishing sites.

The poll of 2,000 adults found 70 per cent have used free public wifi. More than a third have entered passwords, a fifth have used credit cards and 31 per cent have accessed online banking.

“Consumers are choosing convenience over safety when using public wifi,” said Paul Lipman, CEO at BullGuard, which commissioned the study.

“Hackers can easily set up malicious hotspots which appear to be legitimate and yet can intercept and record people’s personal data.

“This allows them to steal usernames, passwords, credit card details, bank account information and more.”

The research also found two thirds of public wifi users have set up their devices to automatically connect to the nearest hotspot – putting their personal details on the line.

Paul Lipman added: “If your device is set up this way, and if you’re not paying attention when you first choose a hotspot, even once, and you accidentally choose something malicious, your device will automatically select it every time it is within range.”

Further to this, four in 10 users habitually connect to hotspots with a name reflecting the location they are in such as “library wifi” or “restaurant wifi”, which can be a risk.

But 62 per cent of respondents were conscious of cyber-crime, and reported being “afraid” of their devices being hacked.

Paul Lipman said: “The findings show that respondents do not feel safe online, yet they are ignoring their fears and are using hotspots without checking they are safe.”

The survey also identified confusion around staying safe when using public wifi – almost half are mistakenly under the impression antivirus software will protect their data.

Paul Lipman added: “Although essential for detecting and removing malware from your device, antivirus offers no protection at all from having your data intercepted by a malicious hotspot.”

“But a Virtual Private Network (VPN) is an effective way of keeping you safe online when using public wifi.

Read the rest here:

https://www.independent.co.uk/life-style/gadgets-and-tech/fake-wifi-hotspots-malware-security-data-warning-a9025441.html

2019 Schedule of Events

Chapter Meetings – Dinner

Tuesday, August 20, 2019

Tuesday, October 15, 2019

Tuesday, November 19, 2019

Chapter Meetings – Lunch

Wednesday, August 21, 2019

Wednesday, October 16, 2019

Wednesday, November 20, 2019

Board Meeting

TBD

Mini-Seminars

Saturday, August 24, 2019

Saturday, October 19, 2019

Saturday, November 23, 2019

Special Interest Group Gatherings (see Page 13)

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, September 3, 2019

Thursday, December 5, 2019

Security +CE Reviews

Saturday, September 14, 2019

Saturday, September 21, 2019

Saturday, September 28, 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:_____________

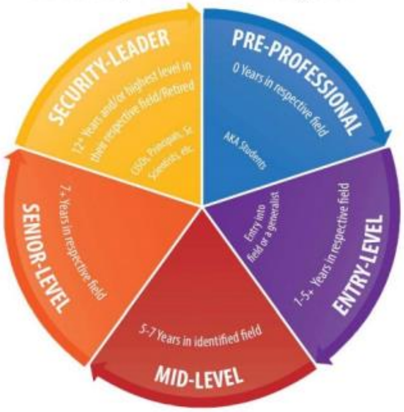
Phone:_____________

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:

May 2019

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

Cybersecurity: Is your boss leaving your organisation vulnerable to hackers?

A survey of security professionals found that over half believe management are ignoring advice designed to help them stay safe from cyberattacks.

By Danny Palmer, ZDNet, July 15, 2019

CEOs and other senior board-level executives are exposing their organisations to cyberattacks and hackers because of a lack of awareness around cybersecurity, a new study has warned.

Research by cybersecurity company RedSeal surveyed hundreds of senior IT and security professionals and found that many of these personnel believe there's a disconnect between the CEO and the information security team, which could be putting organisations at risk.

While almost all security teams (92%) set out specific plans to help protect their CEO from cyberattacks and data breaches, 54% of security personnel believe their CEO is ignoring these plans, potentially opening the door to cyberattacks.

One in ten even went so far as to say decisions or actions made by the CEO or other high-ranking management had actively put the cybersecurity of the business at risk, while 14% said their CEO hasn't received any cybersecurity training.

Meanwhile, 95% of those surveyed said they're concerned that poor cybersecurity of consumer Internet of Things devices means that smarthomes could be hacked – but over a third (38%) aren't aware of which connected devices their CEO uses when they're out the office or at home.

This could potentially provide a new avenue for cyberattackers who want to conduct espionage, steal information or even blackmail high-profile targets.

"Smart devices compete on convenience and price. Security is usually an after-thought, if it's addressed at all. Some popular smart devices, like smart speakers, compromise privacy even when working as intended -- which is scary when you think about the opportunity this presents to people who want to spy on CEOs for commercial or national advantage," said Mike Lloyd, CTO of RedSeal.

"CEOs have wide access to their organisation's network resources, the authority to look into most areas, and frequently see themselves as exempt from the inconvenient rules applied to others. This makes them ideal targets," he added.

However, despite some having fears around security at the very top of the organisation, on the whole, businesses appear to be taking cybersecurity seriously. Two thirds of businesses say their cyber-incident response plan is well defined and well tested – either via real breaches, or simulation tests.

Three quarters of firms also report they have cyber insurance, suggesting there's an awareness around preparing for the aftermath of an incident, should one occur.

Read the rest here:

https://www.zdnet.com/article/cybersecurity-is-your-boss-leaving-your-organisation-vulnerable-to-hackers/

DoD Inspector General Audits Contractor Networks, Systems

By Matthew Nelson, ExecutiveGov, July 29, 2019

The Department of Defense's Office of the Inspector General released the results of an audit that sought to confirm contractors' capacity to secure controlled unclassified information on their respective systems and networks.

The audit confirmed a number of gaps in contractors' security capabilities, including password usage, mitigation of system vulnerabilities and multifactor authentication, DoD OIG said Tuesday.

DoD OIG found that the agency's contracting offices have not developed approaches that will help validate contractual requirements, send contractor notifications, mark CUI documents and confirm implementation of CUI security controls. In addition, the report confirmed that the Defense Threat Reduction Agency did not take prompt action to mitigate the leak of information from a DoD contracting office.

Read the rest here:

https://www.executivegov.com/2019/07/dod-inspector-general-audits-contractor-networks-systems/

Read the report here:

https://media.defense.gov/2019/Jul/25/2002162331/-1/-1/1/DODIG-2019-105.PDF

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.

A Move Toward Transparency: Help Your Tech Staff with an Individual Development Plan

By Paige Reh, CompTIA, July 12, 2019

If you're part of a small business that struggles to find and keep tech talent—something we hear in nearly every CompTIA research report—you should know about one tool I've seen work over and over: an individual development plan (IDP). It's a written document used to assess where people are in their careers, their future goals and how to get here. While there is a wide variety of IDPs, based on different concepts and principles, a good one just came out from CompTIA's Future Leaders Community.

As a human resources professional, I've seen IDPs work as a tool for small business owners and service providers who want to get in touch with their most important resources: their people. Your employees are the No. 1 factor to make or break your organization.

What is an Individual Development Plan?

The Future Leaders IDP helps people identify their professional goals and determine what skills, experiences and behaviors will help achieve those goals. Once all the data is there, you develop and execute an action plan. If there's transparency between workers and management at your company, you can try to help your employees achieve their dreams within your company structure.

Developing a plan doesn't cost a thing, but if you're going to offer certifications or special training to help people reach their goals, it will be an investment. People like to ask, "What if I train my people and they leave?" Consider what happens if you don't train them and they stay.

Why You Should Invest the Time

It can be tough to find a balance between developing employees and managing the daily grind but it's critical for talent attraction, retention and the ultimate success of a business. If you don't take the time to have real and meaningful conversations with your team, do you really think you'll get the results you want at the end of the day?

As a manager or company leader, you've got a perspective on what your employees are good at—whether they know it or not—and you can provide the outsider perspective required to make a self-aware IDP. Follow the guide from CompTIA's Future Leaders and you'll see it can be done in a couple of steps.

1. Start with an honest self-assessment. That includes a non-confrontational discussion about areas of improvement.
2. Help people identify where they want to be in two to five years, and hear the kinds of responsibilities, roles and titles they want to take on. Take that into consideration for your own business plans.
3. Let individuals take the lead on the self-assessment. It should be a reflection on their current knowledge, skills and abilities as they see it. You can help fill in the blanks.

Before you think you can pass this off to HR, understand that you need to look outside of the human resources function to drive performance and make tools like the IDP successful. Employees are accountable for their own performance but should also hold leadership accountable for supporting them along the way.

How It Benefits You

One of the best things you can do as a manager is help people verbalize ways they add value to an organization. Use the Future Leaders IDP to show people how to spin their accomplishments into something another boss will recognize as a good quality—then remember that *you're* the boss and should be allowing employees to lean into those innate skills.

You can also use the IDP as a springboard for effective discussions between employees and their supervisors or teams. This is not a performance appraisal. The conversation should be open and honest with undivided attention from both parties.

A good IDP should be a living, breathing document, a checkpoint or conversation starter that gets re-evaluated every six months. The IDP starts with the individual but it will take management commitment to help drive action.

Read the rest here:

https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2019/07/12/a-move-toward-transparency-help-your-tech-staff-with-an-individual-development-plan?utm_source=Informz&utm_medium=Email&utm_campaign=Membership-FeedOtter-QuickReads%20072219&_zs=8JmMN1&_zl=53uC5

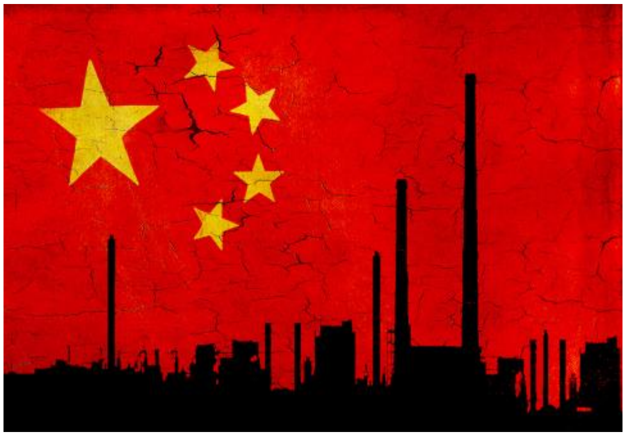
How U.S. Tech Giants are Helping to Build China's Surveillance State

By Ryan Gallagher, The Intercept, July 11, 2018

An American Organization founded by tech giants Google and IBM is working with a company that is helping China's authoritarian government conduct mass surveillance against its citizens, The Intercept can reveal.

The OpenPower Foundation — a nonprofit led by Google and IBM executives with the aim of trying to "drive innovation" — has set up a collaboration between IBM, Chinese company Semptian, and U.S. chip manufacturer Xilinx. Together, they have worked to advance a breed of microprocessors that enable computers to analyze vast amounts of data more efficiently.

Shenzhen-based Semptian is using the devices to enhance the capabilities of internet surveillance and censorship technology it provides to human rights-abusing security agencies in China, according to sources and documents. A company employee said that its technology is being used to covertly monitor the internet activity of 200 million people.



Semptian, Google, and Xilinx did not respond to requests for comment. The OpenPower Foundation said in a statement that it "does not become involved, or seek to be informed, about the individual business strategies, goals or activities of its members," due to antitrust and competition laws. An IBM spokesperson said that his company "has not worked with Semptian on joint technology development," but declined to answer further questions. A source familiar with Semptian's operations said that Semptian had worked with IBM through a collaborative cloud platform called SuperVessel, which is maintained by an IBM research unit in China.

Sen. Mark Warner, D-Va., vice chair of the Senate Intelligence Committee, told The Intercept that he was alarmed by the revelations. "It's disturbing to see that China has successfully recruited Western companies and researchers to assist them in their information control efforts," Warner said.

Anna Bacciarelli, a researcher at Amnesty International, said that the OpenPower Foundation's decision to work with Semptian raises questions about its adherence to international human rights standards. "All companies have a responsibility to conduct human rights due diligence throughout their operations and supply chains," Bacciarelli said, "including through partnerships and collaborations."

Semptian presents itself publicly as a "big data" analysis company that works with internet providers and educational institutes. However, a substantial portion of the Chinese firm's business is in fact generated through a front company named iNext, which sells the internet surveillance and censorship tools to governments.

iNext operates out of the same offices in China as Semptian, with both companies on the eighth floor of a tower in Shenzhen's busy Nanshan District. Semptian and iNext also share the same 200 employees and the same founder, Chen Longsen.

After receiving tips from confidential sources about Semptian's role in mass surveillance, a reporter contacted the company using an assumed name and posing as a potential customer. In response, a Semptian employee sent documents showing that the company — under the guise of iNext — has developed a mass surveillance system named Aegis, which it says can "store and analyze unlimited data."

Aegis can provide "a full view to the virtual world," the company claims in the documents, allowing government spies to see "the connections of everyone," including "location information for everyone in the country."

The system can also "block certain information [on the] internet from being visited," censoring content that the government does not want citizens to see, the documents show.

Aegis equipment has been placed within China's phone and internet networks, enabling the country's government to secretly collect people's email records, phone calls, text messages, cellphone locations, and web browsing histories, according to two sources familiar with Semptian's work.

Chinese state security agencies are likely using the technology to target human rights activists, pro-democracy advocates, and critics of President Xi Jinping's regime, said the sources, who spoke on condition of anonymity due to fear of reprisals.

Read the rest here:

https://theintercept.com/2019/07/11/china-surveillance-google-ibm-semptian/

Security Certification Survey: The high-stakes information security workplace

By Staff, Certification Magazine, July 15, 2018

Security workers have always had an important role in society, but the pay and various working conditions haven't always been above reproach. In the pre-imperial legions of the old Roman Republic, for example, sentries watched the perimeter of the fortified camps every night. A soldier who fell asleep while performing sentry duty could be (and typically was) summarily executed.

One of the most famous security initiatives in history, the building of the Great Wall of China, provides another illustration. During its earliest period of construction, beginning about 221 B.C., the Great Wall was raised by the hands of soldiers, convicts, and peasants, some 400,000 of whom are believed to have died on the job and been unceremoniously interred within the wall itself.

It's a much better time, in 2019, to be a security worker, particularly for those who work with computers and use their skills to defend virtual, not physical, boundaries and battlements. The U.S. Bureau of Labor Statistics estimated last year that there are already 100,000 jobs in the United States for "information security analysts," or individuals who "plan and carry out security measures to protect an organization's computer networks and systems."

Growth in the field over the next 10 years is projected at 28 percent, meaning that an estimated 28,500 more jobs will be created just in the United States by 2026 — a level of expansion described as being "much faster than average." The pay is pretty good, too: BLS research pegs the median annual salary for information security analysts at $98,350, or $47.28 per hour.

What you don't know can hurt you

Even without the looming specter of being executed or worked to death, information security workers have a tough row to hoe. In the course of our recent Security Certification Survey, we asked the more than 420 certified information security professionals who responded to rate their level of agreement with a series of statements about security operations at businesses and other private organizations.

One of the biggest challenges in the field is a people problem. Nearly 83 percent of those surveyed either agree (47.3 percent) or strongly agree (35.6 percent) that enterprise security staffs are too small. The neutral "neither agree nor disagree" middle ground was staked out by 12.7 percent of respondents, leaving a few ticks more than 4 percent who disagree (3.6 percent) or strongly disagree (0.7 percent) that security staffs are too small.

Staffing shortages, however, don't tell the whole story. A perhaps equally telling issue is the general lack of individual security smarts. Slightly more than 75 percent of those surveyed either agree (44.9 percent) or strongly agree (30.3 percent) that employees not hired for technology jobs tend to lack adequate basic information security training.

Even people who are trained to work with computers and information technology (IT) tend not to know as much about security best practices as they should. Three out of every four survey respondents either agree (52 percent of those surveyed) or strongly agree (23.1 percent) that security training of IT personnel on enterprise staffs — those who perform specific IT functions — is not adequate.

The result is that security staffs aren't just contending with outside attacks, but must also continually guard against gaps in the security awareness of their coworkers.

Equipment and spending

On top of manpower challenges and a general lack of security training, most of the certified information security professionals who responded to the survey believe that organizations are bogged down by sketchy software, hardware, and policy protections. More than 62 percent of respondents either agree (48.9 percent) or strongly agree (13.9 percent) that enterprise security controls are lacking.

That's compared to just 12 percent who either disagree (9.9 percent) or strongly disagree (1.8 percent) that controls are not up to snuff. (A further 25 percent of those surveyed signaled a perhaps lesser degree of dissatisfaction with the status quo by choosing to neither agree nor disagree.)

Read the rest here:

http://certmag.com/security-certification-survey-high-stakes-information-security-workplace/

Before Connecting an IoT Device, Check Out a New NIST Report for Cybersecurity Advice

By Staff, NIST, June 27, 2019

Seemingly every appliance we use comes in a version that can be connected to a computer network. But each gizmo we add brings another risk to our security and privacy. So before linking your office's new printer or coffee maker to the internet of things (IoT), have a look at an informational report from the National Institute of Standards and Technology (NIST) outlining these risks and some considerations for mitigating them.

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228) is the first in a planned series of documents NIST is developing to help IoT users protect themselves, their data and their networks from potential compromise. Developed by the NIST Cybersecurity for IoT Program over more than two years of workshop discussions and interaction with the public, NISTIR 8228 is primarily aimed at federal agencies and other big organizations that are incorporating IoT devices into their workplace — organizations that may already be thinking about cybersecurity on a large-scale, enterprise level.

"The report is mainly for any organization that is thinking about security on the level of the NIST Cybersecurity Framework," said Mike Fagan, a NIST computer scientist and one of the authors of the report. "It's targeted at the mode of thinking that an organization would have — more resources, more people, more ability, but also more risk of attack because of all those things. It's bad when a single house is attacked, but if a million bank account passwords are stolen, that has a much larger impact."

Larger organizations may already be using the Cybersecurity Framework and NIST SP 800-53 Rev. 5, two NIST resources that offer guidance for mitigating risk to information systems and the activities that involve them. NISTIR 8228 takes the security and privacy focus from these other documents and considers it in the context of IoT products, from thermostats to voice-operated devices, which may not have traditional interfaces such as a keyboard.

"An IoT device might even have no interface at all, or have no way to install security software," Fagan said. "But it still might connect to your network and be visible electronically to an enemy looking for a potential way in. It's this kind of incongruency with expectations that we want to help an organization think through before they bring IoT devices onto their network."

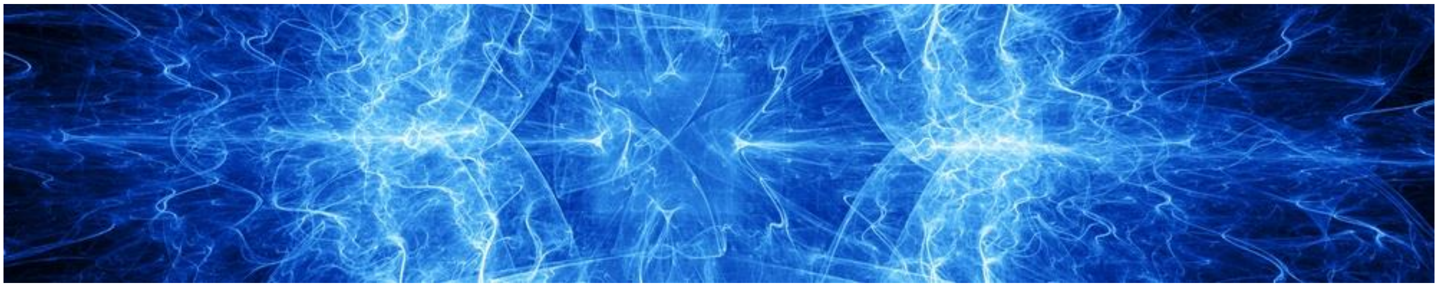
The report is a companion document to the Cybersecurity Framework and SP 800-53 Rev. 5. However, NISTIR 8228 offers only advice; none of its contents are requirements under the Federal Information Security Management Act (FISMA). After distinguishing IoT devices from conventional computers and outlining the type of risks they carry, the authors suggest three high-level risk mitigation goals:

1. **Protect device security,** i.e., prevent an IoT device from being used to conduct attacks;
2. **Protect security of data,** including personally identifiable information; and
3. **Protect individuals' privacy**.

"IoT is still an emerging field," Fagan said. "Some challenges may vanish as the technology becomes more powerful. For now, our goal is awareness."

Specifics are around the corner, though. In the near future, NIST plans to release a core baseline document that aims to identify fundamental cybersecurity capabilities that IoT devices can include. The document will have all IoT devices in mind, including those for individual users and home networks.

"We plan to release a draft of the baseline document for public comment in July, and then we will hold a workshop on August 13 where we will gather feedback," Fagan said. "We'd like to help all IoT users be aware of the risks to their security and privacy and help them approach those risks with open eyes."



Aero Sponsor
CT Cubed
General Membership Sponsor
ter Partner
Colorado Springs Chapter
ISSA
Information Systems Security Association

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

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*

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: **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

How Much Is Your Face Worth? Google Says $5

By Alyse Stanley, Gizmodo, July 29, 2019

How do you train a facial recognition AI reportedly sophisticated enough to rival Apple's Face ID technology? Simple: You offer strangers $5 if they lend you their faces.

At least that's how Google employees went about collecting face scans, according to stories from Android Police and ZDNet that Google confirmed with the Verge today. In various cities across the country, they've been reportedly doling out $5 Starbucks and Amazon gift cards to people on the street in exchange for the totally not creepy request of a few selfies.

Read the rest here:

https://gizmodo.com/how-much-is-your-face-worth-google-says-5-1836803842

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