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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 1 JANUARY 2020

Welcome to 2020!

Fellow Members of ISSA-COS,

Welcome to the year 2020! As the new year kicks off, I hope everyone is ready for a great year of fresh opportunities. Our chapter began planning for 2020 back in October of 2019 and we are excited to finally put those plans into action. This year our chapter seek to enhance the quality of our regularly scheduled events and add several new collaboration opportunities with other organizations in our city and across our state.

Later this month, at each of our January chapter meetings, I will present the **President's Annual Address**. This year, in addition to providing updated statistics about our industry, community, and chapter; I will also provide an overview of the new events and strategic partnerships our chapter has gained for 2020. Accompanying me for these addresses, will be a representative from the National Cyber Exchange (NCX) who will provide us with a technical introduction to the services and capabilities NCX is making available to our members. I have had opportunities to preview these offerings and I am excited they have approached our chapter to partner with them.

A Note From Our President

By Mr. Ernest Campos

In 2020 we will also launch our new quarterly **CyberVIEW Job Fairs**. The first job fair will occur in March and we will need your help securing vendors to attend this event. Participation and registration information will be available soon. Please spread the word and help us institute a success new benefit for our members… insider access to the best new jobs for Cybersecurity professionals in our community.

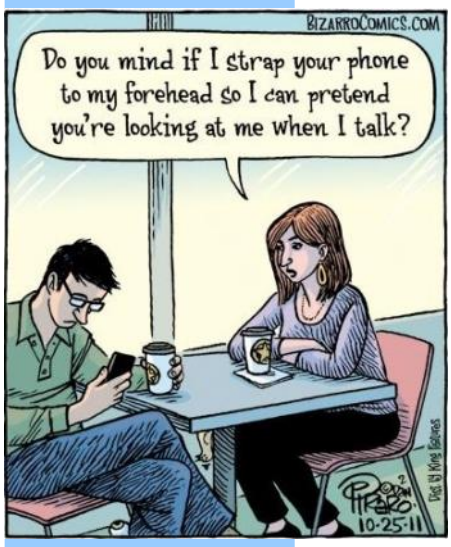
Also, in 2020, we will launch a **new public service program for local Girl Scout troops**. Girl Scouts now have Cybersecurity badges available for them to earn. Our chapter has agreed to develop a program to teach Cybersecurity fundamentals to these scouts, review and reinforce their knowledge, and test their practical comprehension. We will begin with a small pilot group of scouts and will hopefully progress to a full program by the end of the year. Soon, we will request support from folks willing to help develop age appropriate curriculum and ½ day instructors.

Also, also, in 2020, we are partnering with **Women in Cybersecurity** (WiCyS) as they host their annual conference (1500+

(Continued on page 4)

I asked my students to turn in their cell phones and write about living without them

By Ron Srigley, MIT Technology Review, December 26, 2019



A few years ago, I performed an experiment in a philosophy class I was teaching. My students had failed a midterm test rather badly. I had a hunch that their pervasive use of cell phones and laptops in class was partly responsible. So I asked them what they thought had gone wrong. After a few moments of silence, a young woman put up her hand and said: "We don't understand what the books say, sir. We don't understand the words." I looked around the class and saw guileless heads pensively nodding in agreement.

I extemporized a solution: I offered them extra credit if they would give me their phones for nine days and write about living without them. Twelve students—about a third of the class—took me up on the offer. What they wrote was remarkable, and remarkably consistent. These university students, given the chance to say what they felt, didn't gracefully submit to the tech industry and its devices.

"Without their phones, most of my students initially felt lost, but after just two weeks the majority began to think that their cell phones were in fact limiting their relationships with other people."

The usual industry and education narrative about cell phones, social media, and digital technology generally is that they build community, foster communication, and increase efficiency, thus improving our lives. Mark Zuckerberg's recent reformulation of Facebook's mission statement is typical: the company aims to "give people the power to build community and bring the world closer together."

Without their phones, most of my students initially felt lost, disoriented, frustrated, and even frightened. That seemed to support the industry narrative: look how disconnected and lonely you'll be without our technology. But after just two weeks, the majority began to think that their cell phones were in fact limiting their relationships with other people, compromising their own lives, and somehow cutting them off from the "real" world. Here is some of what they said.

"Believe it or not, I had to walk up to a stranger and ask what time it was. It honestly took me a lot of guts and confidence to ask someone," Janet wrote. (Her name, like the others here, is a pseudonym.) She describes the attitude she was up against: "Why do you need to ask me the time? Everyone has a cell phone. You must be weird or something." Emily went even further. Simply walking by strangers "in the hallway or when I passed them on the street" caused almost all of them to take out a phone "right before I could gain eye contact with them."

To these young people, direct, unmediated human contact was experienced as ill-mannered at best and strange at worst. James: "One of the worst and most common things people do nowadays is pull out their cell phone and use it while in a face-to-face conversation. This action is very rude and unacceptable, but yet again, I find myself guilty of this sometimes because it is the norm." Emily noticed that "a lot of people used their cell phones when they felt they were in an awkward situation, for an example [sic] being at a party while no one was speaking to them."

The price of this protection from awkward moments is the loss of human relationships, a consequence that almost all the students identified and lamented. Without his phone, James said, he found himself forced to look others in the eye and engage in conversation. Stewart put a moral spin on it. "Being forced to have [real relations with people] obviously made me a better person because each time it happened I learned how to deal with the situation better, other than sticking my face in a phone." Ten of the 12 students said their phones were compromising their ability to have such relationships.

Virtually all the students admitted that ease of communication was one of the genuine benefits of their phones. However, eight out of 12 said they were genuinely relieved not to have to answer the usual flood of texts and social-media posts. Peter: "I have to admit, it was pretty nice without the phone all week. Didn't have to hear the fucking thing ring or vibrate once, and didn't feel bad not answering phone calls because there were none to ignore."

Read the rest here:

https://www.technologyreview.com/s/614934/teenagers-without-cell-phones/

Membership Corner

Membership Update

Happy New Year! As the new VP of Membership for ISSA-COS, I want to thank Dave Reed for his outstanding service to our chapter as he steps down as the VP of Membership. His commitment to our chapter and fellow members has been beyond reproach. Thank you.

As the new year begins, I kindly ask that all members take the time to update their bio on the ISSA international website. You may do this by logging into the ISSA International website and clicking on the >>Manage Profile link under My Profile. There you will see the "Edit Bio" link where you can make your updates.

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

New Members December
Tundy Fatoye
Matthew Kubiak

Our membership is at ~398 members as of the end of December.

Please watch the Newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. As always, if you have any membership questions don't hesitate to contact me.

Thanks,

Steven Muliz

Membership Committee Chairman

membership@issa-cos.org

Vladimir Putin reportedly runs an outdated version of Windows on his computer that is vulnerable to hacking

By Mary Meisenzahl, Business Insider, December 17, 2019

Russian President Vladimir Putin should update the operating system on his computer. Photos released by the Kremlin showed his computer running an outdated version of Windows, according to The Guardian.

The photos showed Putin's computer was running Windows XP, an operating system that Microsoft stopped updating in 2014, making it more vulnerable to hacking. The risk isn't just theoretical, either. In 2017, ransomware attacked more than 20,000 victims, including the UK's National Health Service, which was using outdated Windows XP software. Hospitals had to close, and operations were even canceled.

Despite the track record of vulnerabilities, Windows XP still had a 2.29% global market share among operating systems as of November, according to NetMarketShare.

The Guardian said the photos showed Putin used Windows XP in his Kremlin office and Novo-Ogaryovo residence outside Moscow. The Russian news website Open Media reported that the Russia's Internet Protection Society head confirmed that the photos showed Windows XP running on both computers.

Read the rest here:

https://www.businessinsider.com/vladimir-putin-uses-windows-xp-on-computer-report-2019-12?utm_source=yahoo.com&utm_medium=referral

(Continued from page 1)

A Note From Our President

attendees!!) in Colorado this year. And we are also partnering with the **National Cybersecurity Center** (NCC) as co-hosts for their annual Cyber Symposium being held in June this year. As you can see, we will have no shortage of opportunities for our members to earn CPEs, share their professional knowledge, and give back to their professions.

In closing, I will leave all of you with a bit of inspiration for the new year. On Page 6 is a statement written by Mr. Kent Keith. Perhaps you have seen before; perhaps you have not. Either way, I ask that you consider it new or anew and adopt the essence of the message as a personal motivator for your year to come. Let 2020 be a year of new starts for yourself. New opportunities. New commitments. New achievements. Let 2020 be the year you own your future, your career, your community, and your chapter.

Let 2020 be the year you **get involved, volunteer, teach, mentor, motivate, represent**… *in ISSA-COS*.

Sincerely,

Ernest

Here's a look back at data breaches in 2019 that occurred due to rogue employees

By Ryan Stewart, Cyware, December 12, 2019

- Rogue employees can exploit the given privileges from the company with a purpose to steal sensitive data about people, processes and intellectual property.
- Capital One, Trend Micro, and Desjardins Group are some of the examples of such data breaches.

Insider threats can bring a massive damage to a company. This malicious threat usually comprises of people associated with an organization such as employees, former employees, contractors, and business associates who have either privileged access or confidential information concerning to the firm.

Rogue or maligned employees can exploit these privileges with a purpose to steal sensitive data about people, processes and intellectual property and give them to whomever they please. The business ramifications of such actions can be incredibly costly. Here's a list of data breaches in 2019 that occurred due to maligned employees.

The top insider breaches in 2019

Capital One suffered a major data leak after an ex-employee of Amazon web services gained access to 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers, and 80,000 bank account numbers by exploiting a misconfigured web application firewall. Apart from Capital One case, Thompson is charged with accessing information of about more than 30 other organizations in and outside the US.

In November, **Trend Micro** disclosed that approximately 70,000 customers were affected after an employee improperly accessed the data with clear criminal intent. The alleged employee sold the stolen information including names and phone numbers to a third party.

Canada's biggest financial services cooperative, **Desjardins Group** took a major decision of reshuffling its management team in the wake of the breach that was disclosed in June. A malign employee associated with the company was fired after he was found to involved in the compromise of the personal data of its 4.2 million members in Quebec and Ontario. The stolen information was shared with third parties outside of the organization.

Read the rest here:

https://cyware.com/news/heres-a-look-back-at-data-breaches-in-2019-that-occurred-due-to-rogue-employees-f8fa4ff9

(ISC)² cert populations for past 12 years

By Kurt Danis, ISSA-COS, 11 December 2019

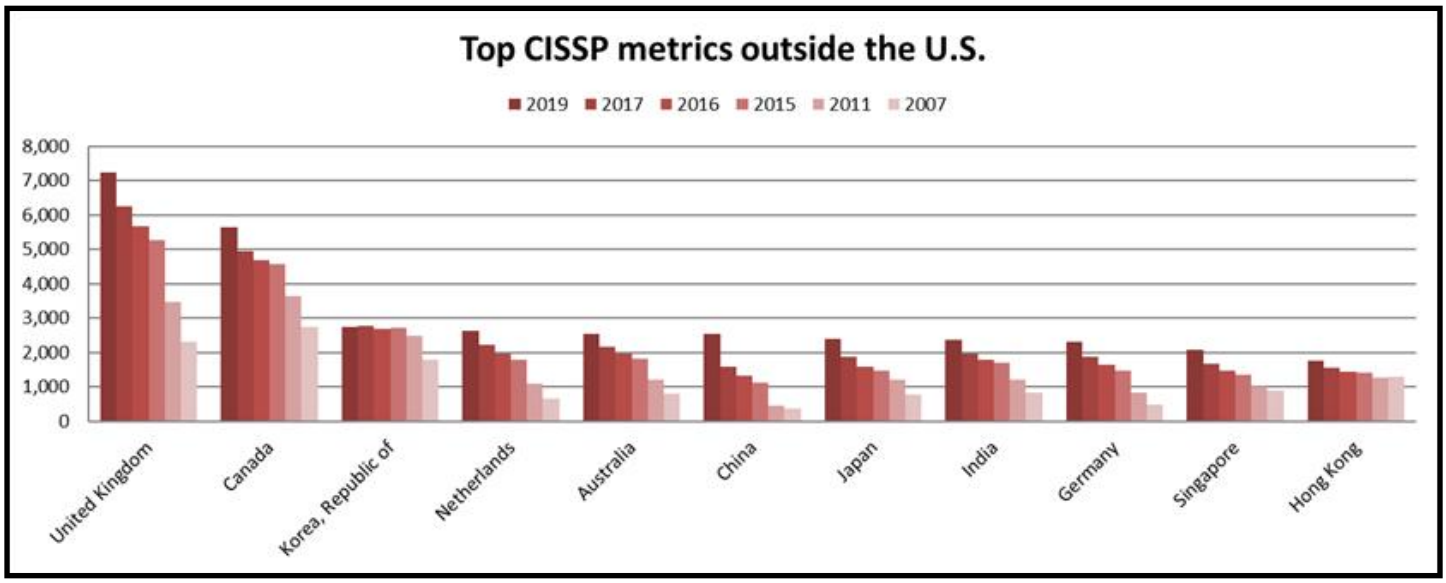
The following numbers represent the top 10 active certifications world-wide offered by the International Information Systems Security Certification Consortium, Inc. (ISC)² as of May 31, 2019.

136,480	CISSP®	Certified Information Systems Security Professional
5,490	CCSP®	Certified Cloud Security Professional
5,408	SSCP®	Systems Security Certified Practitioner
3,162	CAP®	Certified Authorization Professional
2,452	CSSLP®	Certified Secure Software Lifecycle Professional
2,003	ISSAP®	Information Systems Security Architecture Professional
1,293	HCISPP®	HealthCare Information Security and Privacy Practitioner
1,216	ISSMP®	Information Systems Security Management Professional
1,178	ISSEP®	Information Systems Security Engineering Professional
142	CCFP-US®	Certified Cyber Forensics Professional (US)

Next year, the (ISC)² plans to retire the CCFP-US (first introduced in 2013 (p. 6, *InfoSecurity Professional*, Issue Number 22, 2013)). The CCFP will become an "inactive credential" on August 21, 2020. Today, there are 142 CCFP-US holders; a number that hasn't changed much for a few years.

The CCSP, was introduced in 2013. In the past four years, it has more than doubled (5,490 as shown above). The CCSP has surpassed both the CAP and SSCP.

(ISC)² calls the CISSP the "Gold Standard". Today, the US is literally off the chart with 87,343 CISSPs. Most CISSPs hale from English-speaking countries; it is remarkable, that the CISSP population come from 175 countries. Some of the top countries outside the US are shown in the progression bar chart below.



The Paradoxical Commandments

People are illogical, unreasonable, and self-centered.

LOVE THEM ANYWAY.

If you do good, people will accuse you of selfish ulterior motives.

DO GOOD ANYWAY.

If you are successful, you win false friends and true enemies.

SUCCEED ANYWAY.

The good you do today will be forgotten tomorrow.

DO GOOD ANYWAY.

Honesty and frankness make you vulnerable.

BE HONEST ANYWAY.

The biggest men and women with the biggest ideas can be shot down by the smallest men and women with the smallest minds.

THINK BIG ANYWAY.

People favor underdogs but only follow the top dogs.

FIGHT FOR THE UNDERDOGS ANYWAY.

What you spend years building, others will destroy overnight.

BUILD ANYWAY.

People in need of help may strike at you when you offer it.

HELP PEOPLE ANYWAY.

When you give the world the best you have, it will kick you in the face.

GIVE THE WORLD THE BEST YOU HAVE ANYWAY.

Adapted from Kent M. Keith © 1968, 2001

The Year 2019 in Review: Same Threats, More Targets

By Conner Fairman, Council on Foreign Relations, December 10, 2019

In 2019, almost ten years after the discovery of Stuxnet, the United States fell victim to the first cyberattack that disrupted operations in the electrical grid. Cyberattacks on critical infrastructure are becoming increasingly dangerous, yet little has been done to address them. With the modernization of old systems and the introduction of IoT devices and smart city technology, adversaries have a growing list of potential targets to attack. In 2020, governments need to adopt concrete measures to address these threats.

Cyberattacks on critical infrastructure are not a new phenomenon. Discovered in 2010, Stuxnet, a computer worm developed jointly by the United States and Israel that destroyed centrifuges in Iran's Natanz uranium enrichment facility, was the first uncovered malware that affected physical infrastructure. In 2017, malware called NotPetya made headlines for shutting down a fifth of the world's shipping capacity as well as numerous businesses, hospitals, and factories, causing over $10 billion in damages. Finally, in 2019, almost ten years after the discovery of Stuxnet, the United States fell victim to the first cyberattack that disrupted operations in the electrical grid.

Foreign infrastructure also fell victim to cyberattacks this year. In October, India confirmed that malware linked to North Korea's Lazarus Group had infected the networks of Kundankulam nuclear power plant, its newest and largest nuclear power plant. In June, press reports alleged that the United States had penetrated deeply into Russia's electrical grid.

Cyberattacks on the technologies that keep critical infrastructure running appear to have increased in 2019. An April survey of security professionals worldwide tasked with protecting critical infrastructure found that 90 percent had suffered such attacks, with around half of the breaches resulting in the shutdown of critical systems. None of these operations were the "cyber-Pearl Harbor" that some analysts have long warned about, but it is clear that cyberattacks against critical infrastructure are becoming a more dangerous threat.

The threat has increased because of two trends. First, hackers continuously develop more advanced tools, such as Triton, a new malware designed to shut down safety controllers and cause physical damage to critical infrastructure. Second, digitization and the introduction of the internet to systems that predated it has introduced new vulnerabilities. Previously, operational technology was controlled by analog systems, which are kept separate from computer networks, thus insulating it to a degree from malware. With the digitization of these systems, devices that were previously isolated are being connected to the internet, which exposes them to exploitation. Moreover, the widespread implementation of Intenet of Things (IoT) devices throughout facilities has created more targets for would-be attackers. Oftentimes, these devices are easy to exploit, due to the invention of IoT crawlers and factory-set default passwords that are never changed. Thus, companies and governments are inadvertently increasing the attack surface for adversaries.

While security firms are reporting more cyberattacks on critical infrastructure, the providers have, at times, been hesitant to disclose that they have fallen victim. Government operators face political ramifications for admitting that they failed to secure society's most important services. Private utility companies can suffer reputational damage and even expensive fines after admitting that they have been hacked. In some countries, like Germany, operators of some types of critical infrastructure, such as hospitals and public transportation networks, are not obliged to report cyberattacks to authorities. Given the potential consequences of doing so, it is not hard to imagine that attacks in these sectors often go unreported.

Unfortunately for governments and companies, these problems are not going away anytime soon. With the advent of smart city technology, the level of interconnectivity and number of targets that attackers can choose from is going to increase dramatically over the next several years, with particularly large growth expected in Tokyo, New York, and Singapore. Virtually every sector will be affected by this trend, including healthcare, transportation, power distribution, water supply, and public security. Serious vulnerabilities in smart city systems have already been uncovered. For example, in May, security researchers discovered a Chinese database containing facial recognition scans and other personally identifiable information that could be accessed through a web browser without a password. Municipal networks in Atlanta and Baltimore have already been held hostage with ransomware, costing each city millions of dollars. Both cities aspire to become smart cities and have started to implement IoT devices to optimize city processes, such as lighting. Yet, without proper steps to address conventional threats against city networks, these cities' problems will compound, opening the door for an attack that could make the costs incurred from the recent ransomware attacks appear minuscule.

Read the rest here:

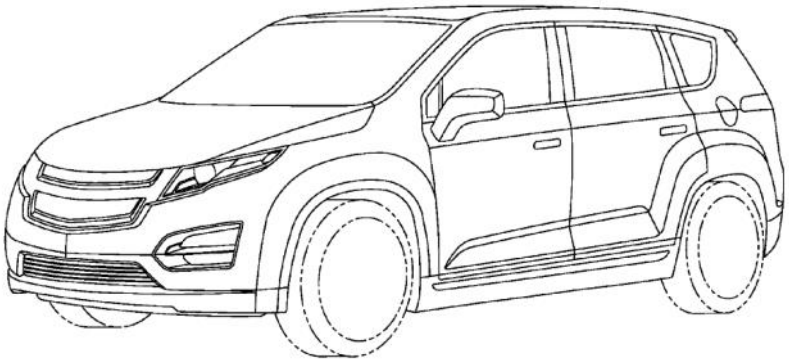
https://www.cfr.org/blog/year-2019-review-same-threats-more-targets

Washington Post Hacked into a Chevy Volt to Show How Much Cars Are Spying on Their Owners

By Sebastian Blanco, Car and Driver, December 17, 2019

It's easy to count up the benefits to connected cars. From using your phone to warm up the cabin on a winter day to setting speed limits for the new teenage drivers in your household, telematics can make life a bit easier. But you're probably not surprised to hear that these upsides come with some potential downsides as well.

This was proven in a big way by *Washington Post* tech columnist Geoffrey Fowler (pictured above), who dug into just how much information his test car, a 2017 Chevrolet Volt, is collecting. Perhaps more important, though, Fowler wanted to see just how much information GM is getting from its connected cars. It's one thing for your car to store your favorite Starbucks in the nav system. It's another if the car company collects that information. The reporter made it clear that this is not a Volt thing, or a Chevy thing; nearly all new cars now have connectivity, including onboard internet connections.



For now, exactly what information goes where is a bit of an unknown by anyone other than the automakers themselves. As Fowler writes, "My Chevy's dashboard didn't say what the car was recording. It wasn't in the owner's manual. There was no way to download it."

To figure this out, Fowler had someone hack into the Volt. He discovered that the car was recording details about where the car was driven and parked, call logs, identification information for his phone and contact information from his phone, "right down to people's address, emails and even photos." In another example, Fowler bought a Chevy infotainment computer on eBay and was able to extract private information from it about whoever owned it before him, including pictures of the person the previous owner called "Sweetie."

While GM was the subject of Fowler's experiments, it's not the only company collecting data on its drivers. In 2017, the U.S. Government Accountability Office looked at automakers and their data privacy policies and found that the 13 car companies it looked at are not exactly using best practices. For example, while the automakers say they obtain "explicit consumer consent before collecting data," the GAO says they "offered few options besides opting out of all connected vehicle services to consumers who did not want to share their data."

GM's OnStar privacy page makes it clear that the company "may use your information to improve the quality, safety, and security of our products and services, to develop new products and services, and for marketing." In response to *Car and Driver*'s request for comment for this article, a GM spokesperson said: "Nothing happens in terms of connected services without customer consent," and also pointed out that collecting vehicle data such as location, vehicle health and status, and operating information "enables many important safety and connectivity services [including] automatic crash notification (alerting first responders to an accident scene), stolen vehicle locator, and vehicle health monitoring (monthly emails to an owner advising them of service and maintenance status)."

"Data is also used to improve vehicle quality and enhance future product designs," the GM spokesman said. The spokesperson also noted that new GM vehicles have a "location services" setting on their center screen, saying, "This allows the driver to switch location services on or off at any time, much like smartphones."

GM also told the *Post*'s Fowler that it will update its privacy policy by the end of 2019.

Currently, No Federal Regulations Are in Place

Data privacy may be a big and growing issue in the automotive industry, but legislators and automakers are moving slowly to tackle it. Fowler points out that there are no federal laws to regulate what automakers can collect or use when it comes to personal driving data. Since 2014, 20 automakers (including GM) have pledged "to meet or exceed commitments contained in the Automotive Consumer Privacy Protection Principles established to protect personal information collected through in-car technologies," according to the Auto Alliance. The first of those principles is to "provide customers with clear, meaningful information about the types of information collected and how it is used," but Fowler's experience shows that this doesn't always happen in the real world.

Read the rest here:

https://www.caranddriver.com/news/a30260730/chevy-volt-hacked-data-collection/

The FY20 National Defense Authorization Act (NDAA) Contains:

Total Funding:

- $738 billion base + Overseas Contingency Operations (OCO)
- $5.3 billion for emergency MILCON funding natural disaster relief

$743.3 billion total

Military Construction for Pike's Peak Region:

- $148 million: Combined Space Operations Facility (CSOF) on Schriever AFB
- $54 million: SOCNORTH on Peterson AFB - https://www.socom.mil/Pages/socnorth.aspx
- $49 million: cadet prep dormitories on USAFA
- $71 million: company operations facilities on Fort Carson

Policy provisions:

- **3.1% pay raise for troops**; includes special pay and bonuses
- Privatized Military Family Housing provisions includes:

⇒ **Establishment of a Tenant Bill of Rights that sets minimum acceptable livability standards**

⇒ Requirement for better communication between Services, providers, and tenants

⇒ Addresses establishment of a formal dispute resolution process

⇒ Bans the use of non-disclosure agreements as a condition of moving out of military housing

⇒ Enhances protections against reprisal.

- **Doubling licensure reimbursement for military spouses**
- **Inclusion of Widow's Tax removal**
- Full funding of nuclear modernization
- Prohibition on transferring Guantanamo Bay detainees to the U.S.
- The NDAA addresses DOD PFAS contamination by:

⇒ Prohibiting non-emergency use of fire-fighting foams containing PFOS and PFOA;

⇒ Requiring DOD to accelerate fielding a PFAS-free replacement;

⇒ Allowing National Guard units to access DOD environmental funds; and

⇒ Requiring expedited cooperative agreements with states.

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.

2020 Schedule of Events

Chapter Meetings – Dinner (5:30 – 7:30 PM)

Tuesday, January 21, 2020
Tuesday, February 18, 2020
Tuesday, April 21, 2020
Tuesday, May 19, 2020
Tuesday, July 21, 2020
Tuesday, August 18, 2020
Tuesday, October 20, 2020
Tuesday, November 17, 2020

Chapter Meetings – Lunch (11:00 – 1:00 PM)

Wednesday, January 22, 2020
Wednesday, February 19, 2020
Wednesday, April 22, 2020
Wednesday, May 20, 2020
Wednesday, July 22, 2020
Wednesday, August 19, 2020
Wednesday, October 21, 2020
Wednesday, November 18, 2020

Mini-Seminars – Breakfast (8:30 – 12:00 PM)

Saturday, January 25, 2020
Saturday, February 22, 2020
Saturday, April 25, 2020
Saturday, May 16, 2020
Saturday, July 25, 2020
Saturday, August 22, 2020
Saturday, October 24, 2020
Saturday, November 14, 2020

ISSA-COS Conferences

Cyber Focus Day (CFD) Symposium

Wednesday, March 25, 2020
Thursday, March 26, 2020

Peak Cyber (PC) Symposium

Wednesday, September 16, 2020
Thursday, September 17, 2020
Friday, September 18, 2020

Security + CE Reviews

Saturday, March 7, 2020
Saturday, March 14, 2020
Saturday, March 21, 2020

Saturday, September 12, 2020
Saturday, September 19, 2020
Saturday, September 26, 2020

CISSP Review

Friday, June 5, 2020
Saturday, June 6, 2020
Saturday, June 13, 2020
Friday, June 19, 2020
Saturday, June 20, 2020
Saturday, June 27, 2020

CyberVIEW Hiring & Networking Fairs (1:00 – 6:00 PM)

Wednesday, March 11, 2020
Wednesday, June 10, 2020
Wednesday, September 9, 2020
Wednesday, December 9, 2020

CyberVIEW hiring and networking events connect Cybersecurity professionals searching for employment with companies looking to fill current or upcoming positions. Soft-skill coaches and resume reviewers will be on hand. This event concludes with a social hour for exhibitors, ISSA-COS members, and guests.

Annual Chapter Celebration (11:00 – 1:00 PM)

Thursday, December 3, 2020

Take time with ISSA-COS to reflect and celebrate the many accomplishments of our chapter from throughout the year. During this event, we will present specific honors, introduce the newly elected board members, and recognize specific professional accomplishments of our general members.

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

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 (WIS)**
- Young Professional in Security – **Y**[oung Professionals]**IS (YIS)**
- Educators in Security – **E**[ducators]**IS (EduIS)**
- Executives in Security – **E**[xecutives]**IS (EIS)**

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 (FIS)**
- Healthcare in Security – **H**[ealthcare]**IS (HIS)**
- Retail in Security – **R**[etail]**IS (RIS)**
- DoD in Security – **D**[oD]**IS (DodIS)**

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
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

ISSA-COS Scholarship Fund Sponsor—ASPG
https://aspg.com/

ASPG
Advanced Software Products Group, Inc.

Update Your Profile!

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

It would take only a stroke of a keyboard to send us back to the dark ages

By John Birmingham, Sydney Morning Herald, December 17, 2019

It's probably not *exactly* true to report, as we did earlier this week, that "Christmas shoppers were left stranded at Myer stores nationwide, unable to pay for items, after a glitch caused registers to shut down for almost three hours".

After all, those shoppers could just walk out. And thousands did.

But the modest hysteria and somewhat restrained chaos of the technological failure was a reminder of just how dependent we've become on the unseen architecture of the digital world.

Bad enough when our phones flake out, or Facebook seizes up. It will be infinitely worse when we collapse the internet for real and on purpose in the opening moments of some future war. Or by accident. Or because some would-be 'Wannacry' scam spins out of control.

It has already happened on a smaller scale. Russian government operators have aggressively targeted smaller, weaker states such as Ukraine for disruption as part of their evolving doctrine of "hybrid war". Unit 61398 of the Chinese Peoples Liberation Army has broken into dozens of Australian businesses, government agencies and educational institutions, sometimes to steal information, sometimes to test for vulnerabilities, and occasionally to set little digital bombs in place, just in case they ever need to collapse our civilisation.

Don't worry, though. We do the same to them.

The digital arms race does raise a possibility you almost never hear spoken of: digital arms control – state-level agreements enforced under treaty to limit the types of cyber weapons that could be used to destroy a modern, technologically advanced economy and severely damage the society that relies on it.

Once upon a time, nations used to negotiate these deals to limit the threat of atomic weapons, or nerve agents, or poison gas. The use of such weapons was considered so dangerous, so heinous, that even implacable enemies were motivated to restrain themselves.

The problem with digital weapons is that you don't need to build factories, or launch sites or whole industries, to support them.

A laptop will do.

So the old saying of "trust but verify", which underpinned the massive reductions in the number of nuclear warheads in the world, doesn't really work as well in the world of ones and zeroes.

It is impossible to verify. Impossible to trust. And so we just keep piling up weaponised code.

Read the rest here:

https://www.smh.com.au/national/it-would-take-only-a-stroke-of-a-keyboard-to-send-us-back-to-the-dark-ages-20191217-p53kn6.html

What is the National Cybersecurity Protection System (NCPS)?

By Jane McCallion, ITPro, December 28, 2019

Founded in 2003 by the United States Computer Emergency Readiness Team (US-CERT), the National Cybersecurity Protection System (NCPS) is a central hub for the analysing potentially malicious cyber activity and if appropriate, formulating a response.

Prior to its founding, federal agencies reported cyber threats directly to the Department of Homeland Security (DHS) on an ad hoc basis – normally once an attack had already happened.

This was inefficient in almost every sense, from the possibility that multiple agencies could be reporting the same thing separately, to the lack of transparency about threats at an inter-agency level, to the fact there was no universal standard or system in place to provide effective network monitoring and defense. NCPS and its operational arm, EINSTEIN, were established to remedy this.

While it's a multi-agency initiative, the NCPS is administered by the DHS through its Cybersecurity and Infrastructure Security Agency (CISA) division. In the words of the agency, NCPS is "an integrated system-of-systems that delivers a range of capabilities, including intrusion detection, analytics, intrusion prevention, and information sharing capabilities" focused on protecting the civilian Federal Government's IT infrastructure (as opposed to military IT infrastructure) from cyber threats. There are four mission areas where the NCPS provides key support capabilities to the wider DHS cybersecurity mission. These are:

- Detection
- Analytics
- Information Sharing
- Prevention

Detection is a signature-based grid that passively monitors networks for potential malicious activity. These signatures are derived from various sources including commercial and public IT security information, as well as information from other federal agencies. The National Cybersecurity and Communications Integration Center (NCCIC) provides another important piece of the puzzle, providing signatures based on analysis it has carried out independently and cybersecurity alerts it has generated. All this is delivered through two elements of the EINSTEIN system – E1 and E2 – which is explored in greater detail below.

Read the rest here:

https://www.itpro.co.uk/security/cyber-security/354443/what-is-the-national-cybersecurity-protection-system-ncps

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

Information Systems Security Association
Colorado Springs Chapter

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:

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

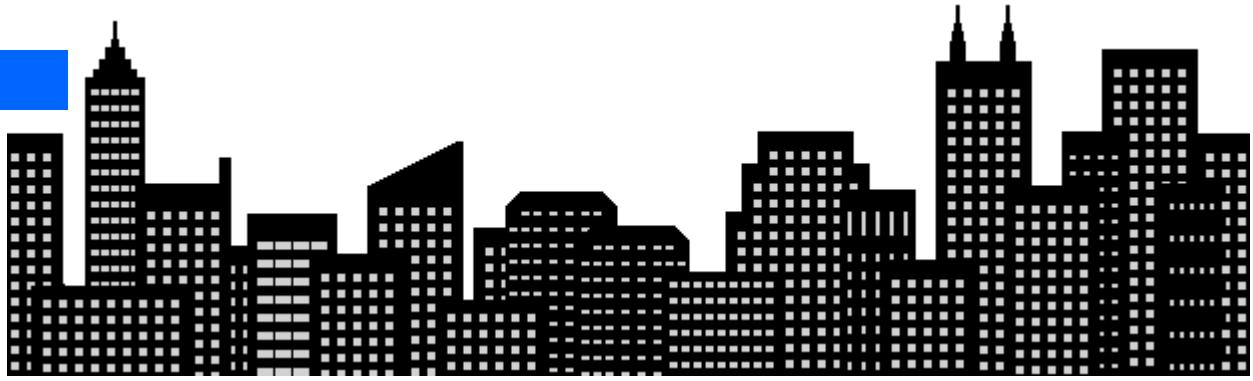
Additional notes:

OFFICE USE ONLY

Follow-up Plan

- ❑ *time recorded*
- ❑ *goals recorded*
- ❑ *resources provided*
- ❑ *referred to SIG:* _____

Next steps:



How to create smart security for smart cities

By Moritz Mann, GCN, December 17, 2019

Smart cities promise greater operational efficiency, increased environmental and financial sustainability and a new level of responsiveness to the needs of residents and visitors. However, this new "intelligence" requires sending information from millions of internet-of-things sensors to the cloud, significantly increasing cybersecurity risks. Governments planning a smart city strategy must accept that they may become a favorite target of attackers.

While most cybersecurity initiatives focus on preventing attacks, cyber defenses will never be perfect because they depend on humans doing the right thing -- and attackers know how to prey on human vulnerabilities, including carelessness, fear and a desire to respond to pleas for help. So while working to minimize the risk of attack, governments must develop a resilient infrastructure that minimizes the impact of breaches.

Successful cybersecurity requires good cyber hygiene and effective cybersecurity practices. Instead of pretending their patients will never get sick, doctors recommend minimizing the risk of sickness through good hygiene -- frequent hand washing, eliminating bacteria around the house, etc. -- then bolstering patients' defenses with healthy practices, such as eating well and exercising. This way, inevitable illnesses tend to have less impact.

Today, most government agencies rely on multiple-point solutions to block cyberattacks. While many of these products are excellent, the disconnect between the individual solutions creates security gaps. Effective cyber hygiene requires a single, centralized solution for managing and protecting the entire network. For several years, companies have used software-defined wide-area networking to centralize and simplify network management. In 2019, Gartner defined a new solution category: secure access service edge (SASE), which combines an SD-WAN with network security services.

The goal of SASE is to inspect traffic *once* and apply consistent policies across the entire infrastructure, including at the edge and across multiple clouds. It eliminates the complexity of applying policies as data crosses separate network borders, which often creates security and compliance vulnerabilities. The SASE inspects all traffic without latency and consistently applies security measures -- such as next-generation firewalls, intrusion-detection and anti-malware scanning -- all according to the agency's policies.

A SASE that is delivered as an end-to-end fully managed service also eliminates the need to constantly upgrade, patch and rethink every aspect of the network. Instead, the as-a-service delivery model increases network flexibility, scalability, security and performance, while optimizing IT resources.

While a SASE can establish basic cyber hygiene, smart cities must still practice "a healthy lifestyle." This includes putting the right people and processes in place to minimize risk. For example, because human error is a common cause of breaches, agencies train everyone who handles data on their individual responsibilities for protecting that data, including securing social media and email accounts, backing up data where required, keeping all devices and applications not managed by the agency up to date and learning to avoid phishing and spear-phishing scams.

Many agencies have made great strides in promoting these healthy practices; however, most still ignore perhaps the most important cyber defense preparation: a robust incident response (IR) plan that can minimize data loss, the financial impact and the time to restore processes and services.

An effective IR plan requires:

- *Preparedness* – Build a quality IR team. Security engineers should have the technical skills to uncover and defend against attacks, as well as the social skills to connect with colleagues when a breach occurs. Team members may also include compliance officers, human resources managers, attorneys and public relations specialists. The team should be involved in helping to develop cyber policies and an IR communications plan to ensure timely delivery of information to internal and external stakeholders.

Read the rest here:

https://gcn.com/articles/2019/12/17/sase-smart-city-security.aspx

What's 5G, And Why Are People So Scared of It? Here's What You Really Need to Know

By Jacinta Bowler, Science Alert, January 1, 2019

Earlier this year the Belgian government halted a 5G test over radiation concerns. Switzerland is monitoring risks posed by the 5G network. A member of the UK House of Commons warned the parliament of the "unintended consequences" of the 5G upgrade.

5G fears have become mainstream. But their point of origin is anything but.

If you go digging into the claims behind these fears, you'll discover some truly wild conspiracy theories. Some people claim that 5G is in the same wavelengths as weapons. Or that it's being used by the military to break the enemy's spirit.

People have argued that the smaller wavelengths used in each new generation of mobile phone infrastructure have never been tested, and therefore we are guinea pigs for this technological experiment. By and large, claims about the harms of 5G are not far from gay frog conspiracies.

You'll be happy to know that none of those claims are true.

"The wavelengths that 5G uses and will use are all entirely safe and have been in research and testing for decades," Howard Jones, the head of technology communications at UK's mobile network provider EE, recently explained to *The Guardian*.

"It's a red herring to say it's a new technology and therefore hasn't been tested."

There's an awful amount of terror out there over a phone network. Chances are many people couldn't explain what 5G even is, so here's a brief overview of the actual technology.

When you use your phone, it interacts with a phone tower nearby, via radio waves. The phone tower then connects (also via radio waves) to a core network, which then passes on the information it receives and sends information back.

Currently, if your phone uses 4G, the frequency band of the radio waves it employs is anywhere from 2 - 8 GHz. This is a slightly higher frequency than 1.8 – 2.5 GHz for 3G (and can be slightly different, depending on your region).

Using higher frequencies has both advantages and disadvantages. The higher the frequency of a radio wave, the shorter the wave itself. Similarly to sound waves, shorter waves lose energy faster as they move, so they cover less distance.

The area covered by the phone tower - also known as a base station - is called a 'cell', and these are usually around 1 to 20 kilometres wide, although they can be a lot smaller, depending on how many phones there are in the area.

At weaker frequencies, one tower covers less area, therefore you need more towers. However, shorter waves also mean that many more devices can be connected to one phone tower at once. 5G potentially offers network connection speeds that will be substantially higher than what's currently available.

Read the rest here:

https://www.sciencealert.com/why-are-people-so-scared-of-5g

It's Time to Nervously Mock the 50 Worst Passwords of the Year

By Catie Keck, Gizmoto, December 18, 2019

In spite of everything—the leaks, the breaches, the myriad privacy risks—a large majority of people are still using “password” and “123456” as their password. Folks, it’s long past time to stop taking security shortcuts.

Security services firm SplashData has released its ninth annual Worst Passwords of the Year list, which assesses more than 5 million leaked passwords to determine those most commonly shared by hackers. This year’s list has revealed that people are still using easily guessable and common passwords to guard their data, including those frequently cited in past reports as being particularly susceptible to attacks.

While “password” fell two spots on this year’s list compared to last year’s, it remains in the top five—along with “123456" and “123456789.” There are some newcomers to the list, such as “qwertyuiop” and various repeated number sequences like “7777777,” however the report notes that even passwords that appear complicated are rather created using keys situated next to each other on the keyboard. It adds that these types of passwords “may seem to be complex but will not fool hackers who know millions of people use them.”

Behold, the worst of the worst:

Read the rest here:

https://gizmodo.com/its-time-to-nervously-mock-the-50-worst-passwords-of-th-1840514905

WWW.ISSA-COS.ORG

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

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

Article for the Newsletter?

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

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Chapter Officers:

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

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

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

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: Steven Mulig
- Deputy: Melissa Absher

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

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

Committee Chairs:

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

Executive Assistant: Andrea Heinz

** Executive Board Members*

Past Senior Leadership

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

How the KGB Bugged American Typewriters During the Cold War

By Kyle Mizokami, Popular Mechanics, January 1, 2020

The Cold War spy drama that played out between the U.S. and the Soviet Union was the source of much ingenious spy technology. One of the most ingenious devices fielded by both sides was a typewriter designed to spy on the user, quietly transmitting its keystrokes to KGB listeners. The technology was an early form of keylogging but done entirely through hardware—not PC software .

Read the rest here:

https://www.popularmechanics.com/military/a30370413/typewriter-bugging-cold-war/

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