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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 10 NUMBER 4 APRIL 2021

April—*Finally!*

Welcome to April showers! As I write this article, we find ourselves in the beginning of Spring. New life is beginning to abound all around us… and yes, even within our own chapter. As we embark on the 2nd quarter of the year, we look forward to many returning events lost last year due the pandemic. We also look forward to the start of some new annual events. And let us not forget the triumphant return of the Cyber Focus Symposium! Indeed, Spring is in the air!

A Note From Our President

By Mr. Ernest Campos

Before we discuss all the great opportunities that lie ahead, let us quickly look back and review the month of March. Last month, our chapter hosted the first of our two virtual Security + Reviews. Over the course of three consecutive Saturdays, approximately 35 people invested their personal time towards achieving their professional goals. I was excited to see so may new participants during my opening comments for the review. I am grateful for all the chapter members who volunteered to polish the curriculum and serve as instructors and facilitators. The feedback I received from participants is that the review provided excellent opportunities to learn and comprehend some rather complicated material. For all those who participated, I wish you luck on your upcoming exams!

In March, our chapter successfully rolled out a multi-month effort to update our website. Have you seen it? We fancy! The updated website better profiles our chapter, our sponsors, upcoming events, and member benefits. It is a face-lift our chapter greatly needed and one that showcases our chapter in a more professional way. Yes folks, we have arrived, and the view is spectacular! Here again, I took pause to appreciate the tireless efforts of our IT Committee, chaired by **Mr. Pat Sheehan**, and the services of **Colorado Web Impressions** (www.coloradowebimpressions.com), owned and operated by **Mr. Chris Heidlebaugh**, who graciously volunteered his services to assist us in this effort. The benefits of an updated website will greatly enhance the image of our chapter and will help foster new sponsorships and strategic partnership. The intrinsic value of this upgrade will reap

(Continued on page 4)

Mumbai's Electrical Blackout: Chinese Gray-Area Warfare?

By Austin Bay, On Point, March 2, 2021

Let's start with relevant facts. Mumbai is India's largest city (20 million residents), its major financial center (India's central bank is located there) and the capital of the state of Maharashtra, a financial powerhouse unto itself.

Those facts alone make Mumbai a target for any group seeking to weaken India, much less wage war on India. For example, damaging a financial hub exacts immediate and long-term economic costs.

"The October Mumbai blackout perfectly fits the uncertain and deniable criteria."

That's why Pakistani-backed Islamic terrorists have launched several attacks on the city. In 2006, terrorists blew up packed commuter trains. In November 2008, an Islamic terrorist assault team attacked Mumbai and murdered 166 people.

Here are some newer facts only Big Lie propagandists would dispute, but there are a lot of those snakes around: At 10 a.m. on Oct. 12, Mumbai suffered a massive electrical power outage. Local trains stopped, stranding passengers. Cellphone service crashed. India's bond market was disrupted during peak trading hours. Some neighborhoods lost power for over 12 hours. Indian media called the outage Mumbai's "worst in decades." And it was.

In November, India Today reported that Maharashtra's cyber department believed a malware attack could have caused the crippling outage. "Could have" is speculation, not fact. However, technical experts found indications of attempted cyber intrusions on digital devices controlling Mumbai's grid.

On Feb. 28, The New York Times reported Recorded Future, a Massachusetts-based company that -- get this anodyne description -- "studies the use of the internet by state actors," had discovered Chinese malware "flowing into the control systems that manage electric supply across India" and elsewhere in the electrical production and transmission system.

Caveat: Because Recorded Future could not get inside India's complex power grid, its experts could not examine the malware's details.

A further qualification: On March 2, IndiaTimes.com reported that India's Union power minister, R.K. Singh, said there is no evidence a cyberattack caused Mumbai's blackout. The power ministry believed human error caused the outage, not cyberattacks by China or Pakistan.

New caveat: The ministry agreed there were attempted cyberattacks on India's northern and southern region electric control centers, but the malware did not reach the operating systems.

Additional caveat of confusion: On March 1, Maharashtra's home minister, Anil Deshmukh, claimed that the Mumbai power outage in October 2020 was a cyber-sabotage attempt.

Observation: In democratic nations, national and state governments/politicians frequently contradict one another because they really don't know. I offer Dr. Anthony Fauci as an example of a politician who contradicts himself.

Bottom-line fact: The Sino-Indian War of 1962 is still unresolved. In 2020, Indian and Chinese military forces repeatedly squared off in the Himalayas. During one 2020 military confrontation in the Galwan Valley, Maharashtra state authorities noticed an increase in Chinese attempts to penetrate its power grid.

Bottom-line fact: Chinese-sourced malware entered the Indian digital network associated with the electrical power grid.

Read the rest here:

https://strategypage.com/on_point/20210302213335.aspx

Membership Corner

Membership Update

Have you updated your contact information on the ISSA International website? You have! That is awesome. If you have not, please log onto the ISSA International website and click on your welcome icon on the top of the page and select "Account + Settings". Once there you can make your updates. Thank you for your support.

We need all members to spread the word that we are looking for new members to join our great organization. Below are the top 10 reasons join ISSA!

Top 10 Reasons Cybersecurity Professionals Join ISSA

1. Build professional relationships
2. Learn practical/best practices solutions
3. Keep up on developments in information security/risk/ privacy
4. Career information and employment opportunities
5. Content of chapter meetings
6. Advance the profession
7. Professional development or educational programming offerings
8. Give back to the profession
9. Earn CPEs/CPUs
10. Develop the next generation of cybersecurity professionals

Our membership is hanging in at ~341 members as of the end of March 2020. Please watch the newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. As always, if you have any membership questions don't hesitate to contact me or Craig Westerfield, Deputy VP-Membership.

Thanks,

Craig Westerfield

VP-Membership
membership@issa-cos.org

New Members March 2021	
Kevin Johnson	Robert "Bob" Turner
Jon Martin	

CISA Strongly Urges All Organizations to Immediately Address Microsoft Exchange Vulnerabilities

Original release date: March 8, 2021

CISA has published a Remediating Microsoft Exchange Vulnerabilities web page that strongly urges all organizations to immediately address the recent Microsoft Exchange Server product vulnerabilities. As exploitation of these vulnerabilities is widespread and indiscriminate, CISA strongly advises organizations follow the guidance laid out in the web page. The guidance provides specific steps for both leaders and IT security staff and is applicable for all sizes of organizations across all sectors.

A Note From Our President

(Continued from page 1)

countless benefits for our chapter for many years to come. It is for this reason we are proud to recognize Colorado Web Impressions as a new Platinum sponsor based on the financial value of their no-cost services to our chapter.

Now, looking forward towards April, we will enjoy an earlier than normal monthly chapter meeting as we give way later this month for other events. This month, we will host a panel discussion devoted towards unraveling the breach of the SolarWinds Orion software product. For this event, we have scheduled some heavy hitters within our industry who will help breakdown the events that led to a monumental security breach that affected hundreds of public and private sector businesses and organizations. Make sure you sign up to attend – you will not want to miss it.

Also in April is the return of our annual **Cyber Focus Symposium**. This event was cancelled last year just 2-weeks before the onset of the pandemic within our region. Since we still find ourselves navigating the pandemic, we made an early decision to host the CFS as a virtual event; especially given the incredible success of the virtual Peak Cyber Symposium held in November of 2020. This year's CFS will include the return of **Ms. Halie E. Anthony**, Missile Defense Sector Director, Boecore, Inc. as our Master of Ceremonies. Prominent keynote and guest speakers for this event will include:

- **Mr. Benjamin Edelen** – Chief Information Security Officer (CISO), City of Boulder, Colorado
- **Mr. Dave Sonheim** – Cybersecurity Advisor, Region VIII, CISA, Department of Homeland Security
- **Mr. William Hoffman** – Chief Information Officer (CIO), FrontLine Cyber Solutions
- **Ms. Charity Wright** – Cyber Threat Intelligence Analyst, Recorded Future

As a reminder, the CFS will include a free virtual job fair hosted by **Cleared Careers** and a free Boss-of-the-NOC CTF hosted by **Splunk** and **Epoch Concepts**. As always, registration for the symposium is FREE for members of ISSA (any chapter) and anyone with a (dot) mil, (dot) gov, or (dot) edu email address. Registration is required to attend, and early registration is especially appreciated. For more information on speakers, sponsorship opportunities, registration, or scheduled events, please browse to www.cyberfocusdayco.com. Please help promote this event by spreading the word throughout your social and community circles. ISSA-COS extends special thanks to **Mr. Dennis O'Neill** and his team from **Secret Sauce Events** (http://www.secretsauceevent.com) for their production, promotion, and hosting of this virtual event – *Dennis, you da man!*

Later this year in mid-June, our chapter will host the inaugural **Cyber SIG Summit**; a half-day, afternoon event where we will showcase our many different Special Interest Groups (SIGs). Each SIG will host a 1-hour presentation for participants to attend. Immediately following this event, ISSA-COS will host a community wide **Cyber Social** where Cyber-related organizations from across our region will gather to share valuable information while networking with attendees. At this event, ISSA-COS will also celebrate our 30th anniversary!! Thirty years! Wow, that is like 10-years times three!

In closing, our chapter is in full swing with lots of events happening and even more to come. Please consider attending as many events as you can and please remember to bring a friend, co-worker, or student. New faces are always welcome. Final gratitude goes to all our chapter members who continue to make ISSA-COS the *best* chapter in the world.

Sincerely,

Ernest

Instructions & Credit for Online Playbacks of ISSA-COS Training Sessions

- Video playbacks are available to ISSA-COS members within 3-days
- Navigate to the www.issa-cos.org website
- Login using your *COS Chapter* credentials
- Navigate to "Training" and select the desired month
- Select the desired presentation and enjoy the playback
- Upon completion of the playback, email: certification@issa-cos.org and identify the *month* and *session number* for the episode you viewed.

Book Report

By Jay Carson, Security+, CIPP/E, Semper Sec LLC, ISSA-COS Member-at-Large

Our 2020 ISSA-COS chapter meeting presenters recommended these two books:

Another of the neat things about attending ISSA-COS events is you get references to excellent books about different aspects of cybersecurity. For example, at the recent Security+ Review, the presenter talked about a "scary" book:

Watts, Clint. *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. Harper Paperbacks, 2019 (originally published 2018).

I immediately ordered it on Amazon, and this is ***not*** the book to read just before you go to bed! A cybersecurity professional like you will never get to sleep! Oh, the book is plenty interesting, all right. The author is credentialed and experienced, the writing style comfortable, the publication fairly current. Mr. Watts has testified multiple times before Congress, and you may have seen him on television news programs speaking as an expert. The original date of publication was 2018, with the edition I read having an epilogue dated 26 Dec 2018. There are lots of good footnotes referencing other books and articles, particularly on mass psychology. The Pikes Peak Library District has multiple copies, or you can get a used copy on Amazon for under $12 including shipping. It is a great book to read with your morning coffee, when you can deal with the challenges of the day.

I headed the ISSA-COS Speakers Bureau Committee for two years, and I do not think we ever had a speaker that took defenses against hacking quite as far in this direction. As I said, his footnotes and references are extensive. In my opinion, he did his homework.

The book focused on two types of villains, first terrorists, then nation-states, specifically the Russians as they attempt to thwart US interests.

Hey Jay! Enough already about the book!
What is in the book? What makes it scary?

What about hackers that want your brain and the brains of others? That scary enough? I am not talking about 'brain' in the anatomical sense. I am talking about brain as the sum total of all you think, feel, and how you act. Call it mind control if you prefer. For a cybersecurity professional, this book is a real-life horror movie!

We are all quite challenged already by hackers that are after financial data, health records, or other personal information. We know about ransomware attacks. We know about hacking for the purpose of disruption or physical damage to infrastructure systems. How about foreign actors that hack into social media to gather enough information on you to manipulate you for their benefit? The manipulation is to slowly change, through flooding you with fake but just-believable information, your political beliefs. The manipulation is what they have learned based on your social media history of affinities. According to Mr. Watts' research, the Russians are masters of the psychological art, and they just keep getting more skilled. Mr. Watts does not leave you on edge. He gives defensive advice for the nation based on his long experience.

I am not going to spoil the book for you with all Mr. Watts' examples. However, one non-social media example struck a nerve with me, and there are other sources like Wikipedia where you can read the details. He summarizes the hack of the 2016 U.S. Democratic candidate's emails, by the hacker (Fancy Bear, a.k.a. the Russians) sending an email disguised as a Google security alert to the campaign chair with link stating a password needed to be reset. I know you are thinking, "OK, that is classical spear-phishing." The target sent the email to IT to check, and IT sent back "legitimate" when meant "**il**legitimate." You know what happened! And this is Carson's soapbox. Everyone, your Mom, your kids, anyone on the internet needs to be aware of just how easy it is to be hacked even when you think you are taking precautions. Cyber hygiene for everyone!

Happy reading!

America's Drinking Water Is Surprisingly Easy to Poison

By Peter Elkind, ProPublica, March 17, 2021

On Feb. 16, less than two weeks after a mysterious attacker made headlines around the world by hacking a water treatment plant in Oldsmar, Florida, and nearly generating a mass poisoning, the city's mayor declared victory.

"This is a success story," Mayor Eric Seidel told the City Council in Oldsmar, a Tampa suburb of 15,000, after acknowledging "some deficiencies." As he put it, "our protocols, monitoring protocols, worked. Our staff executed them to perfection. And as the city manager said, there were other backups. ... We were breached, there's no question. And we'll make sure that doesn't happen again. But it's a success story." Two council members congratulated the mayor, noting his turn at the press conference where the hack was disclosed. "Even on TV, you were fantastic," said one.

"Success" is not the word that cybersecurity experts use to describe the Oldsmar episode. They view the breach as a case study in digital ineptitude, a frightening near-miss and an example of how the managers of water systems continue to downplay or ignore years of increasingly dire warnings.

The experts say the sorts of rudimentary vulnerabilities revealed in the breach — including the lack of an internet firewall and the use of shared passwords and outdated software — are common among America's 151,000 public water systems.

"Frankly, they got very lucky," said retired Adm. Mark Montgomery, executive director of the federal Cyberspace Solarium Commission, which Congress established in 2018 to upgrade the nation's defenses against major cyberattacks. Montgomery likened the Oldsmar outcome to a pilot landing a plane after an engine caught fire during a flight. "They shouldn't celebrate like Tom Brady winning the Super Bowl," he said. "They didn't win a game. They averted a disaster through a lot of good fortune."

The motive and identity of the hackers, foreign or domestic, remain unknown. But Montgomery and other experts say a more sophisticated hacker than the one in Oldsmar, who attempted to boost the quantity of lye in the drinking water to dangerous levels, could have wreaked havoc. They're skeptical of the city's assurances that "redundant" electronic monitors at the plant protected citizens from any possible harm. "If the attackers could break into the lye controls," Montgomery said, "don't you think they could break into the alarm system and alter the checkpoints? It's a mistake to think a hacker could not introduce contaminated water into our water systems." Oldsmar officials, citing the ongoing investigation, declined ProPublica's requests for an interview or to address emailed questions about the city's cybersecurity practices.

The consequences of a major water system breach could be calamitous: thousands sickened from poisoned drinking water; panic over interrupted supplies; widespread flooding; burst pipes and streams of overflowing sewage. (This is not merely theoretical. In 2000, a former municipal wastewater contractor in Australia, rejected for a city job, remotely manipulated computer control systems to release 264,000 gallons of raw sewage, which poured into public parks, turned creek water black, spilled onto the grounds of a Hyatt Regency Hotel and generated a stench that investigators called "unbearable." The man was sentenced to two years in prison.)

In congressional testimony on March 10, Eric Goldstein, cybersecurity chief for the federal Cybersecurity and Infrastructure Security Agency, described the Oldsmar incident as illustrating "the gravest risk that CISA sees from a national standpoint." He said it should be "a clarion call for this country for the risk that we face from cyberintrusions into these critical systems."

Grave warnings have sounded for years. As far back as 2011, a Department of Homeland Security alert advised that hackers could gain access to American water systems using "readily available and generally free" internet search tools. Such admonitions have abounded in recent years. Booz Allen Hamilton's 2019 "Cyber Threat Outlook" called America's water utilities "a perfect target" for cyberattacks; a 2020 Journal of Environmental Engineering review found "an increase in the frequency, diversity, and complexity of cyberthreats to the water sector"; and the Cyberspace Solarium Commission's March 2020 report warned that America's water systems "remain largely ill-prepared to defend their networks from cyber-enabled disruption."

Despite the warnings, and some high-profile breaches dating back a decade, the federal government has largely left cyberdefense to the water utilities. For years, it relied on voluntary industry measures, dismissing any need for new regulation. Then, in 2018, Congress included a provision addressing cybersecurity in a 129-page water bill that covered everything from river levee repairs to grants for school water fountains.

Read the rest here:

https://www.nextgov.com/cybersecurity/2021/03/americas-drinking-water-surprisingly-easy-poison/172749/

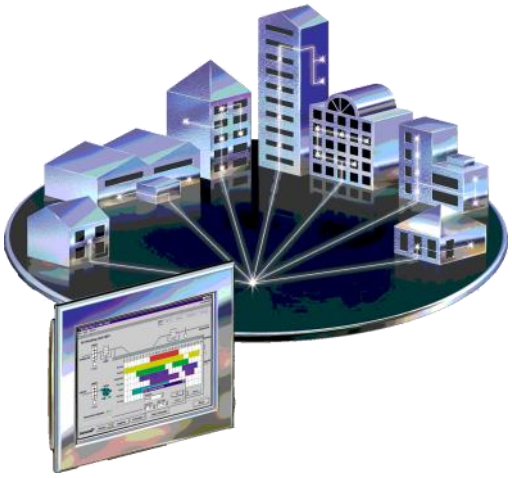
STIG SCADA Security in a Cellular World

By Noa Ouziel, Security Boulevard, March 21, 2021

SCADA systems have been around since the early 1970s, way back when networks were all closed systems and hacking them was the stuff of spy movies. All this changed in the early 2000s when those networks became exposed to the internet. The increased connectivity allowed for higher productivity, access, and simplicity of use. However, with **higher connectivity came new security concerns, as well as industry standards for protecting critical SCADA networks**.

With the rise of cellular communication for industrial applications and Industry 4.0? It was only a matter of time before the adoption became global. High speeds, low costs, and a solution for SCADA networks that need to cover large distances all make cellular an ideal connectivity choice. However, increased wireless connectivity introduced additional attack vectors threatening the operation and safety of the devices connected.

Are those attack vectors enough to slow down the adoption of cellular connectivity for SCADA networks?



What are SCADA networks?

SCADA interfaces can also allow for input, which means that the factory floor manager can not only get data but also make adjustments. In some cases, the SCADA system itself can make automated adjustments based on sensor data, saving many staff and managers' work hours.

Wireless connectivity

To this day UHF (Ultra High Frequency) Radio is the gold standard for safe and easy wireless connectivity. But it's easy to see why it is being phased out as part of digital transformation of industrial networks. **UHF is generally limited to a bandwidth of 19.6 kbps, which is more than enough to transfer commands to connected devices, but falls short when attempting to collect large amounts of DATA** or even a single CCTV feed. Moreover, UHF radio is unreliable, relatively slow and prone to interference.

Alternatives to UHF radio for wireless connectivity for SCADA networks vary. **A Wi-Fi router can replace UHF radio, but that won't hold up along very large distances**. Another older industrial connectivity solution are satellite connections. **The problem with satellite connectivity is that it is very costly, and latency can become an issue** with critical system controls.

Radio frequencies and Wi-Fi can suffice for some SCADA networks, especially when there is only a need for low-level diagnostics and basic commands. But **when more data needs to be transferred, and scalability is a goal one solution stands tall above the rest — cellular connectivity**.

Private cellular networks in particular are a very affordable way to get long-distance connectivity as long as a cellular tower is in range. A **public cellular network can offer a less reliable and secure option by connecting to the Internet, but offloads many related costs and maintenance concerns**. In either case, you wouldn't need much more than a cellular modem at every endpoint.

SCADA on IIoT

IIoT, the Industrial Internet of Things, is **the collective name for devices connected to the Internet in industrial applications**. Some devices have the built-in capability to connect to the Internet on their own through a built-in cellular modem component. Others use a local network as a gateway to the WAN (be it the Internet or an Intranet).

Generally speaking, **anything that can connect to SCADA can connect to the Internet via a central computer**. Connecting devices to the Internet allows managers to employ the power of cloud computing and big data processing to give a much deeper understanding of the systems connected.

With the power of IIoT comes the vulnerability to external cyber-attacks. Where SCADA networks are a closed Intranet system by design, **IIoT is exposed to the public Internet**. Cybersecurity of devices connected to the Internet is a well-developed field, but **SCADA brings its own set of vulnerabilities. That is, before we even mention the contribution of wireless connectivity** to the overall attack surface of any industrial network.

Read the rest here:

https://securityboulevard.com/2021/03/scada-security-in-a-cellular-world/

2021 ISSA International Annual Awards Nominations are now OPEN!

Suspense for submissions is 16 May 2021

Every year ISSA International recognizes excellence in information security professionals, the companies they work for, and the chapters to which they belong.

The Colorado Springs Chapter has won numerous ISSA International awards over the years and we hope to continue that amazing trend! Our chapter has two members on the Hall of Fame and six members on the Honor Roll. We've won Chapter of the Year three times, Security Professional of the Year twice, President's Award for Public Service once, and Volunteer of the Year FIVE years in a row!

We need your help in identifying individuals to nominate for the awards described below. If you'd like to recommend someone for any award, please contact the Past Presidents at: past-president@issa-cos.org by the end of March. Additional info about each award can be found on the ISSA International website at: https://www.issa.org/issa-international-awards-2021/?utm_source=WordPress&utm_medium=Organic&utm_campaign=Informz

ISSA International Awards 2021 - ISSA International

Awards Nomination Open on February 15, 2021 (Awards Nomination Now Open). Will close on May 16th, 2021. Hall of Fame is a lifetime achievement award recognizing an individual's exceptional qualities of leadership in their own career and organization as well as an exemplary commitment to the information security profession. Honor Roll is a lifetime achievement

Hall of Fame is a lifetime achievement award recognizing an individual's exceptional qualities of leadership in their own career and organization as well as an exemplary commitment to the information security profession.

Honor Roll is a lifetime achievement award recognizing an individual's sustained contributions to the information security community, the advancement of the association and enhancement of the professionalism of the membership.

The **Security Professional of the Year** honors one (1) individual who best exemplifies the most outstanding standards and achievement in information security in the preceding year.

The **Volunteers of the Year** Award recognizes a member who has made a significant difference to their chapter, the association or the information security community through dedicated and selfless service to ISSA.

The **Organization of the Year** Award recognizes candidates with a sustained, proactive presence that directly contributed to the overall good and professionalism of the association and its membership, providing either services, products and/or direct support that ensures the promotion of the highest ethical standards in addressing information security and its future direction.

Chapter of the Year recognizes chapters that have done an exceptional job of supporting ISSA's mission, serving their member communities and advancing the field. Award are given in small, medium, and large chapter categories.

The Power of Positive Thinking

By Andrea Heinz, ISSA-COS Recorder, March 8, 2021

Everyone is aware that positive thinking can bring many benefits to their lives. Positive thinking can increase your energy levels by causing your body to release endorphins – mood elevating chemicals within the brain. It can improve your physical health by reducing the release of the hormone, cortisol, that can contribute to stress, anxiety, depression, high blood pressure, heart disease, and a host of other health issues.

Positive thinking can enhance your performance at your job by encouraging you to believe in yourself, set goals, and maintain the focus needed to achieve those goals, and it can improve your relationships with family, friends, and coworkers by contributing to a positive attitude that results in more positive interactions and outcomes with everyone. Positive thinking can improve your life in a great number of ways.

One of the best things about positive thinking is that it is relatively effortless to achieve - and it is absolutely free! You can become a more positive thinker by "training your brain" to start focusing on the positive instead of the negative.

Take time regularly to practice some of the tips listed below to start your journey down the road to becoming a more positive thinker and to begin enjoying a happier and healthier life!

- Practice positive self-talk.
- Get regular exercise and maintain a healthy diet.
- Pursue a hobby or passion!
- Set goals.
- Help others!
- Be grateful!
- Find the positive in all situations!
- Read motivational books.
- Practice meditation.
- Surround yourself with positive people!
- Get plenty of rest.
- Don't forget to see the humor in life!

"A positive mind finds opportunity in everything. A negative mind finds fault in everything." – **Unknown**

Update Your Profile!

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

Strategic Partnership

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Comments/Questions: INFO@ISSA-COS.ORG 3

Murray Security Services Sponsorship

- $2,500 per quarter = $10,000 commitment
- 4 **CODERED** Licenses to be provided as give-always at ISSA-COS Events ($1000 value)
- $1000 off (preferred pricing) on most all MSS Professional Training & Certification courses. (no-one else receives this type of standard discount)
- Providing 2 (free) training classes later this summer. Value: $5,000. C|TIA & ESCA

Comments/Questions: INFO@ISSA-COS.ORG 4

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING

EC-Council
Hackers are here. Where are you?

ISSA Colorado Springs Chapter

EC-Council CODERED

CODERED is EC-Council's subscription-based learning platform which allows you to access bite sized content through a clean, simple learning platform!

- **Premium Content:** 4000+ Premium Videos
- **Fresh Content:** New courses and content are added weekly to our library to keep you up-to-date with the latest skills and technologies.
- **Practical Content:** The courses published on **CODERED** contain an abundance of demo lab videos that dive deeper into important cyber concepts and gives you the practical technical knowledge you need to advance your career and improve your performance as a cyber professional.

Comments/Questions: INFO@ISSA-COS.ORG 5

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING

EC-Council
Hackers are here. Where are you?

ISSA Colorado Springs Chapter

Certified Threat Intelligence Analyst (C|TIA)

The Certified Threat Intelligence Analyst (CTIA) program is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe.

The aim is to help organizations hire qualified cyber intelligence trained professionals to identify and mitigate business risks by converting unknown internal and external threats into quantifiable threat entities and stop them in their tracks.

Reducing Cybersecurity Risk With Minimal Resources

By Dan Lohrmann, Government Technology, March 6, 2021

How can organizations protect critical information resources? What processes and procedures work best? What are the challenges to reducing risk?

To answer these questions and much more, I turned to a cybersecurity industry thought leader from Texas: Mike Davis.

Mr. Davis is the CISO in alliantgroup's Houston national office, where he operationalizes data security, privacy and risk management while advising leadership on protecting critical information resources and managing an enterprise cybersecurity portfolio. Mike and his team's mission includes executing a risk-based security strategy that supports enabling the company's success objectives by securing and protecting both sensitive company and client information and resources.

Before joining alliantgroup, Mike was the CISO of a large global maritime classification company. He is an experienced cybersecurity professional with 20-plus years in several environments (commercial, military and government) and diverse leadership positions: CISO, senior cyber technical authority, cybersecurity/risk management consultant, cyber program manager and chief systems engineer, among others. Mike is also a retired U.S. Navy Engineering Duty Officer and federal government employee (GS-15).

Mike supports several professional associations: the FBI InfraGard, IEEE (Life Member) and ISSA/ISC2, among others. His certifications are: CISSP, CISO and Systems Engineering, along with senior qualifications in Program Management and Risk Management, and he holds a master's in electrical engineering and in management.

I have known Mike for several years, and he always brings insightful, thought-provoking content and insights to complex cyber discussions.

Dan Lohrmann (DL): What are the biggest cybersecurity risks most enterprises face?

Mike Davis (MD): To start our risk journey, we need to all have an overall risk assessment baseline — assess our vulnerability baseline and the top threats applicability to our environment. We use a periodic sampling approach from the many threat reporting sources (as part of our "CTI" program), then distill those results into the following current risk areas that we sense apply to most organizations:

- Phishing: Over 90 percent of all security incidents start here (where someone will always "click"!)
- Ransomware, including morphing malware/crypto-mining: It's easy and profitable, *and now comes with a data breach extortion threat too*.
- Poor cyberhygiene: known vulnerabilities not patched (98 percent of exploits use these)
- Ineffective access controls: Identity is the new perimeter and core (ZTA) (e.g., we need multifactor authentication everywhere)
- Hostile intruders: hackers, insider threats, careless users, any malicious user
- Crime as a service: as now anyone can be a hacker, just pay the criminals
- Internet of Things security: the many atypical computing devices connected to your network
- Third-party/vendor access and risks: this is a major threat all by itself and accounts for half of all breaches
- Regulation/compliance (e.g., GDPR, SOX, PCI DSS, etc.): Fines, loss of integrity/brand and competitiveness.

Overall, start with a risk assessment to set your baseline tailoring threats and associated mitigations to your organization, develop a clear risk-value-based risk reduction plan, with OPS/IT concurrence (as they will need to support many). Then get understanding from your IT/risk steering committee (ITSC), to then do the same with senior leadership. This in an older two-page article that goes into the question overall: "Cyber risk, what really matters?"

By the way, if you are interested in which mitigations to focus on first, skim this article on the hierarchy of cybersecurity needs from Microsoft; it follow's the Maslow hierarchy of needs triangle, with a cyber perspective. The foundation is access control, and each layer is well described.

DL: How do you think about attacking the problem of reducing risk?

Read the rest here:

https://www.govtech.com/blogs/lohrmann-on-cybersecurity/reducing-cybersecurity-risk-with-minimal-resources.html

Cybersecurity in 2021: Stopping the madness

By Eric Knarr, CSO Online, March 8, 2021

Marc Andreessen had it right – software has eaten the world. As a result, the world can be hacked.

Just look at the past few months. The SolarWinds caper – the "largest and most sophisticated attack the world has ever seen" according to Microsoft president Brad Smith – gave its Russian perps months of free reign across untold US government agencies and private companies. But stupid also works: Last month in Florida, a water treatment plant's cybersecurity was so lax, anyone could have been behind a clumsy attempt to poison the local water supply. Meanwhile, miscreants bearing ransomware have made hospitals their favorite target; in October 2020, six US hospitals fell prey within 24 hours.

Cybersecurity wins the award for Most Dismal Science. But if suffering attacks now amounts to a cost of doing business, then the time-honored approach of prioritizing risk and limiting damage when breaches occur still offers reason for hope. This collection of articles from CSO, Computerworld, CIO, InfoWorld, and Network World delivers specific guidance on best security practices across the enterprise, from the C-suite to developer laptops.

Writing for CSO, contributor Stacey Collette addresses the age-old question of how to focus upper management's attention on security in "4 ways to keep the cybersecurity conversation going after the crisis has passed." The thesis is that five-alarm debacles like the SolarWinds attack can serve as useful wakeup calls. Collette suggests seizing the moment to convince the board to match the company business model with an appropriate risk mitigation framework – and to use information sharing and analysis centers to exchange information on industry-specific threats and defensive measures.

CIO's contribution, "Mitigating the hidden risks of digital transformation" by Bob Violino, surfaces a problem hiding in plain sight: Digital innovation almost always increases risk. Everyone understands the transformative power of the cloud, for example, but each IaaS or SaaS provider seems to have a different security model, raising the odds of calamitous misconfiguration. Likewise, digital integration with partners promises all kinds of new efficiencies – and by definition heightens third-party risk. And does it even need to be said that launching an internet of things initiative will vastly expand your attack surface area?

A second story written by Violino, this one for Computerworld, explores the cybersecurity obsession of our era: "WFH security lessons from the pandemic." Some of the article covers familiar ground, such as ensuring effective endpoint protection and multifactor authentication for remote workers. But Violino also highlights more advanced solutions, such as cloud desktops and zero-trust network access. He warns that a new wave of preparation will be required for hybrid work scenarios, in which employees alternate between office and home to ensure social distancing at work. The pandemic has proven that remote work at scale is viable – but new solutions, such as pervasive data defense and response platforms, will be necessary to secure our new perimeterless world.

Read the rest here:

https://www.csoonline.com/article/3610369/cybersecurity-in-2021-stopping-the-madness.html

Hackers are finding ways to hide inside Apple's walled garden

By Patrick Howell O'Neill, MIT Technology Review, March 1, 2021

You've heard of Apple's famous walled garden, the tightly controlled tech ecosystem that gives the company unique control of features and security. All apps go through a strict Apple approval process, they are confined so sensitive information isn't gathered on the phone, and developers are locked out of places they'd be able to get into in other systems. The barriers are so high now that it's probably more accurate to think of it as a castle wall.

Virtually every expert agrees that the locked-down nature of iOS has solved some fundamental security problems, and that with these restrictions in place, the iPhone succeeds spectacularly in keeping almost all the usual bad guys out. But when the most advanced hackers do succeed in breaking in, something strange happens: Apple's extraordinary defenses end up protecting the attackers themselves.

"It's a double-edged sword," says Bill Marczak, a senior researcher at the cybersecurity watchdog Citizen Lab. "You're going to keep out a lot of the riffraff by making it harder to break iPhones. But the 1% of top hackers are going to find a way in and, once they're inside, the impenetrable fortress of the iPhone protects them."

Read the rest here:

https://www.technologyreview.com/2021/03/01/1020089/apple-walled-garden-hackers-protected/

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING

EC-Council
Hackers are here. Where are you?

ISSA Colorado Springs Chapter

EC-Council Certified Security Analyst (ECSA): Penetration Testing

The ECSA penetration testing course provides you with a real-world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available.

It covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

Comments/Questions: INFO@ISSA-COS.ORG 7

ISSA Colorado Springs Chapter

Upcoming Events

April Chapter Meeting – 4/6/2021

- Chapter Announcements
- Technical Presentation

April Mini Seminar – 4/10/2021

- Technical Training
- Hands-on Tools and Techniques

Cyber Focus Symposium (CFS) – Apr 20, 21, and 22, 2021

- CFS Job Fair: *Sponsored by Cleared Careers*
- CFS CTF: *Sponsored by Splunk> and Epoch Concepts*
- CFS Conference: *Produced by Secret Sauce Events*

Annual Cyber SIG Summit – Jun 18, 2021

- Eight (8) Special Interest Groups (SIGs) profiled
- Half-day event; 1PM – 5PM

Annual Cyber Social – Jun 18, 2021

- No cost to attend; Free to all Community Partners
- ISSA-COS 30th Anniversary Celebration

Comments/Questions: INFO@ISSA-COS.ORG 10

(Continued on page 9

ISSA Information Systems Security Association Colorado Springs Chapter

Social Media

- **Twitter**
  - Colorado Springs ISSA
  - @COSISSA
  - https://twitter.com/COSISSA
- **LinkedIn**
  - ISSA Colorado Springs Chapter
  - https://www.linkedin.com/groups/1878203/
  - https://www.linkedin.com/in/issa-cos-7495361b2
- **Facebook**
  - Colorado Springs Chapter of the ISSA
  - @ColoradoSpringsISSA
  - https://www.facebook.com/ColoradoSpringsISSA
- **Instagram**
  - issa_cosprings
  - https://www.Instagram.com/issa_cosprings/

Comments/Questions: INFO@ISSA-COS.ORG

ISSA-COS SALUTES ALL OUR CURRENT **COMMUNITY PARTNERS!**

THANK YOU FOR ALL YOU DO TO SUPPORT OUR CHAPTER AND OUR COMMUNITY!

TOGETHER WE ARE STRONGER

WWW.ISSA-COS.ORG

Microsoft Attack Blamed on China Morphs Into Global Crisis

By William Turton and Jordan Robertson, Bloomberg, March 6, 2021

A sophisticated attack on Microsoft Corp.'s widely used business email software is morphing into a global cybersecurity crisis, as hackers race to infect as many victims as possible before companies can secure their computer systems.

The attack, which Microsoft has said started with a Chinese government-backed hacking group, has so far claimed at least 60,000 known victims globally, according to a former senior U.S. official with knowledge of the investigation. Many of them appear to be small or medium-sized businesses caught in a wide net the attackers cast as Microsoft worked to shut down the hack

The European Banking Authority became one of the latest victims as it said Sunday that access to personal data through emails held on the Microsoft server may have been compromised. Others identified so far include banks and electricity providers, as well as senior citizen homes and an ice cream company, according to Huntress, a Ellicott City, Maryland-based firm that monitors the security of customers, in a blog post Friday.

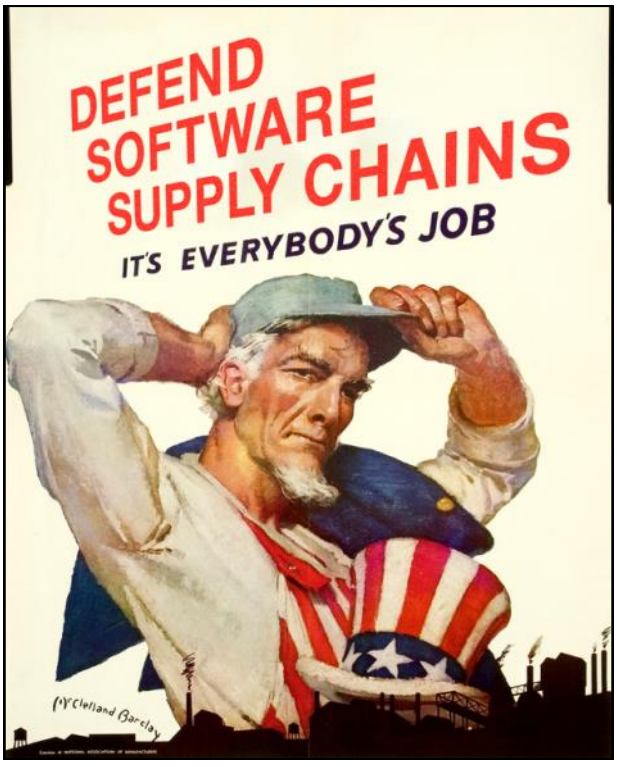
One U.S. cybersecurity company which asked not to be named said its experts alone were working with at least 50 victims, trying to quickly determine what data the hackers may have taken while also trying to eject them.

The rapidly escalating attack came months after the SolarWinds Corp. breaches by suspected Russian cyberattackers, and drew the concern of U.S. national security officials in part because the latest hackers were able to hit so many victims so quickly. Researchers say in the final phases of the attack, the perpetrators appeared to have automated the process, scooping up tens of thousands of new victims around the world in a matter of days.

Washington is preparing its first major moves in retaliation against foreign intrusions over the next three weeks, the New York Times reported, citing unidentified officials. It plans a series of clandestine actions across Russian networks -- intended to send a message to Vladimir Putin and his intelligence services -- combined with economic sanctions. President Joe Biden could issue an executive order to shore up federal agencies against Russian hacking, the newspaper reported.

Read the rest here:

https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world



ISSA-COS Sponsorship Plans

ISSA-COS Annual Financial Sponsorship Packages	Platinum	Gold	Silver	Bronze	Single Event
	$19,995	$14,995	$9,995	$4,995	$2,495
Name/Logo recognition in the following channels					
a. Chapter website	X	X	X	X	X
b. Mass-marketing emails	X	X	X	X	X
c. Monthly newsletter	X	X	X	X	X
d. On-screen recognition at scheduled events	X	X	X	X	X
Preferred Guest Speaker for the following events					
a. Cybersecurity Special Events	X	X	X	X	X
b. Chapter Meetings and Mini Seminars	X	X	X		
c. Cyber Focus Symposium	X	X			
d. Peak Cyber Symposium	X				
Discounted Exhibitor Packages for conferences					
a. Cyber Focus Symposium: 5' x 8' (Full Price: $1,495)	-$500	-$400	-$300	-$200	-$100
b. Peak Cyber Symposium: 5' x 8' (Full Price: $1,495)	-$500	-$400	-$300	-$200	-$100

Material Sponsors		
Type	Qty	Fee
Training Vouchers	12	$12,000
Shirts	250	$4,000
Padfolios	250	$2,200
Lapel Pins	250	$800
Book Bags	250	$400
Notepads	250	$200
Pens	250	$150
Stickers	250	$100
Logo Socks	250	$2,500
Logo Beanies	250	$3,000
Sponsor's Choice	250	TBD
Venue/Facility	n/a	$0

Comments/Questions: SPONSORSHIPS@ISSA-COS.ORG 1

Mentorship

Executives of U.S. technology companies told lawmakers on February 23 that a recent breach of corporate and government networks was so sophisticated that a nation had to be behind it and said all the evidence points to Russia.

Read the rest here:

https://www.rferl.org/a/russia-hack-computer-technology-us-government/31118886.html

Mentorship is a relationship between two people, a mentor, and a mentee. A mentor is an experienced and knowledgeable individual who passes their knowledge and experience to a mentee so they may gain a solid footing into their chosen career field. This relationship is an extremely valuable tool for both the mentor and the mentee.

For the mentee, it provides invaluable insight into building a successful career by which the mentor helps the mentee establish measurable short- and long-term goals that are attainable and relevant for their chosen information system security career field. For the mentor, it provides an opportunity to lead and develop our future generation of information system security specialists. This partnering relationship is essential for providing knowledge, advice, motivation, and encouragement for successful mentee development and positive information system security career field growth.

Did you know that ISSA-COS has a mentorship program? Well, it is true! ISSA-COS has a mentorship program and we are looking for mentors that are wanting to contribute to developing our future generation of information system security specialists. We are also looking for a mentorship committee chair to lead our mentorship program. If you are interested in volunteering to be a mentor or are interested in leading our ISSA Mentorship Committee, please contact memberservices@issa-cos.org.

Steven Mulig
ISSA-COS, VP-Membership

Craig Westerfield
ISSA-COS, Deputy VP-Membership

MENTORING PROGRAM

The ISSA-COS Mentoring Program provides a connection between individuals (mentees) seeking career guidance, industry information, or personal encouragement with individuals (mentors) who have an aptitude for sharing their career experiences, industry resources, and personal talents for the benefit of the mentee. Mentees derive from every conceivable background and exist at every stage of professional development. Mentoring sessions are designed to ensure the confidentiality, integrity, and availability of information shared between the participants.

To help facilitate the mentoring process, ISSA-COS has adopted the S.M.A.R.T. goal setting model to safeguard a consistent development process that is equally understood and honored by mentees and mentors alike. As such, the Mentoring Program supports the following objectives of ISSA-COS:

For more information about mentoring, email: *mentorship@issa-cos.org*

- Promote increased professional education opportunities for members
- Provide career guidance and professional development approaches
- Encourage balance between technical skillsets and soft skills such as time management, task management, workplace conduct, and business savvy
- Increase member knowledge of available resources designed to strengthen skillsets
- Encouraging an open exchange of Cybersecurity related techniques, approaches, and problem-solving skills
- Promote member education and awareness of Cybersecurity security issues and recommended strategies to combat the issues
- Providing opportunities for mentees and mentors to network with other professionals and share their lessons learned from their individual mentoring experiences.

Cyber Spotlight – PARTY!!

ISSA-COS is turning 30 in 2021!

Initiative to document ISSA-COS Chapter History

Interviews with past/current **Presidents**

Interviews with past/current **Board Members**

Interviews with past/current **General Members**

Interviews with **Community Partners**

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: Craig Westerfield
- Deputy: **Vacant**

Vice President of Training: Jeff Tomkiewicz
- Deputy: Phebe Swope

Member at Large 1: Art Cooper
Member at Large 2: Jim Blake
Member at Large 3: James Asimah
Member at Large 4: Jay Carson

Committee Chairs:

Annual Audit: Chris Edmondson
Training: Mark Heinrich
Mentorship Committee Chair: Carissa Nichols
Media/Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson
Girl Scouts Cyber Badge Camp: Anna Parrish
Annual Election: Colleen Murphy

**** 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

Zoom Escaper lets you sabotage your own meetings with audio problems, crying babies, and more

By James Vincent, The Verge, March 15, 2021

Had enough Zoom meetings? Can't bear another soul-numbing day of sitting on video calls, the only distraction your rapidly aging face, pinned in one corner of the screen like a dying bug? Well, if so, then boy do we have the app for you. Meet Zoom Escaper: a free web widget that lets you add an array of fake audio effects to your next Zoom Call, gifting you with numerous reasons to end the meeting and escape, *while you still can*.

Read the rest here:

https://www.theverge.com/2021/3/15/22331744/zoom-escaper-sabotage-meetings-fake-audio-problems

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