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

ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 9 SEPTEMBER 2020

Colorado Springs, Colorado

The Return of *Anonymous*

By Dale Beran, The Atlantic, August 11, 2020

At the end of may, as protests against the police killing of George Floyd got under way, reports started to circulate that the shadowy hacker group Anonymous was back.

The rumors began with a video depicting a black-clad figure in the group's signature Guy Fawkes mask. "Greetings, citizens of the United States," the figure said in a creepy, distorted voice. "This is a message from Anonymous to the Minneapolis Police Department." The masked announcer addressed Floyd's killing and the larger pattern of police misconduct, concluding, "We will be exposing your many crimes to the world. We are legion. Expect us."

The clip generated a wave of renewed enthusiasm for Anonymous, particularly among young people. Twitter accounts associated with the group saw a surge of new followers, a couple of them by the millions.

At the height of its popularity, in 2012, Anonymous had been a network of thousands of activists, a minority of them hackers, devoted to leftist-libertarian ideals of personal freedom and opposed to the consolidation of corporate and government power. But after a spate of arrests, it had largely faded from view.

Now a new generation was eager to join. "How does one apply to be a part of Anonymous? I just wanna help out, I'll even make the hackers coffee or suttin" an activist in the United Kingdom joked on Twitter, garnering hundreds of thousands of likes and retweets.

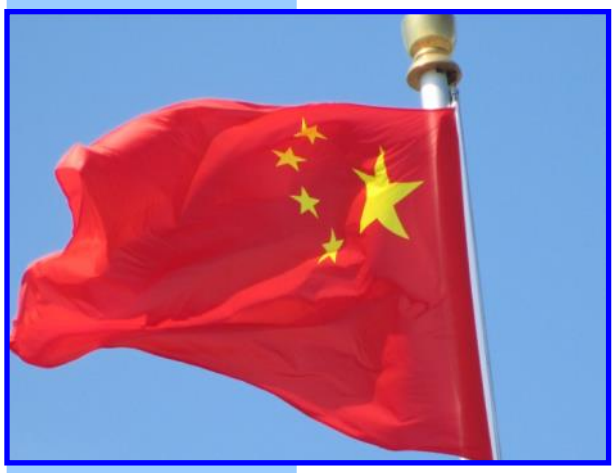
Anonymous "stan" (super fan) accounts remixed the video on TikTok to give the shadowy figure glamorous nails and jewelry. Others used the chat service Discord to create virtual spaces where thousands of new devotees could celebrate the hackers with memes and fan fiction. One of the largest Anonymous accounts on Twitter begged people to "stop sending us nudes."

A series of hacks followed the release of the video. News outlets speculated that it was Anonymous who had hijacked Chicago police scanners on May 30 and 31 to play N.W.A's "Fuck tha Police" and Tay Zonday's "Chocolate Rain," a 2007 song that served as an unofficial anthem for the group. Likewise, when the Minneapolis Police Department website went offline from an apparent DDoS attack—a hack that overwhelms a target site with traffic—social media credited

(Continued on page 4)

Is China the World's Greatest Cyber Power?

By Robert Lemos, Dark Reading, August 27, 2020



While China-linked groups continue to target cyberattacks against specific industries to steal intellectual property and against government agencies to steal political secrets, the Chinese government has broaden both its techniques and its strategies, which — along with its aggressive operations — has made the country "perhaps the world's top cyber power," threat intelligence firm IntSights states in its latest report published on August 27.

"Overall, the group exhibits significant technical capabilities, using 150 different malware components from almost 50 code families ..."

The nation's aggressive approach to using cyber operations to achieve political and national aims has set its cyber strategy apart from the more cautious and considered approaches of most other nations. Attackers linked to China have vacuumed up personally identifiable information on US and European citizens, stolen trade secrets and intellectual property, and exfiltrated classified information from government agencies, all without much political impact to the Chinese government. As China's goals shift to broaden its reach worldwide, more of its effort has focused on the suppression of foreign and domestic opponents that are critical of the Chinese Communist Party, according to IntSights' "Dark Side of China: The Evolution of a Global Cyber Power" report.

The US government has already designated China as the nation's top cyber adversary. And China will only increase its focus on cyber, says Etay Maor, cybersecurity expert and chief security officer at IntSights. China's last Five-Year Plan, published in 2016, stated that the government would direct the country's manufacturing toward more innovative products from low-value goods — an obvious motivation for the country's continued attacks, he says.

"When it comes to China, cyber is not a tactical weapon, it is a strategic means to an end," Maor says. "And if you are wondering what that end is, it is not something secret — it is something that is published every five years."

As part of the broader focus on the world stage, Chinese cyberattackers will likely continue to expand their scope of targets. In the past, the US and European targets bore the brunt of cyberattacks from China-linked groups, but increasingly attacks are driven by the country's ambitions elsewhere, the report states. India, Australia, and attacks on specific cultural and religious groups have suffered numerous attacks in the past few years.

"Over the past decade, China has become increasingly forthright in its intentions, and this change has been observed in cyber operations as well," the report states. "Researchers have observed stark differences in tactics, tone, and behavior from Chinese state-sponsored cyber, military, and political parties over the past several years."

While some security experts may argue that the United States, or even Russia, should be considered the world's greatest cyber power — especially, if cyber is considered to be more than just cyber operations — the argument that China takes the top slot is not idle.

In a press briefing in July, FBI Director Christopher Wray called Chinese cyberattacks targeting US companies' intellectual property and gathering up the personal information of US citizens as "one of the largest transfers of wealth in human history." The FBI placed the blame on China for the 2017 hack of Equifax, which stole the personal data on 150 million Americans and noted that half of the 5,000 counterintelligence investigations currently being conducted in the United States are related to China.

Read the rest here:

https://www.darkreading.com/threat-intelligence/is-china-the-worlds-greatest-cyber-power/d/d-id/1338778?&web_view=true

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.

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

New Members August
Drew Koch
David J. Berkowitz
Lynn Burns
Kirsten Mullican
Jasmine C. Nichols
Brian Pumilia

Our membership is hanging in at ~354 members as of the end of August 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.

Thanks,

Steven Mulig

Vice President of Membership

membership@issa-cos.org

(Continued from page 1)

Anonymous.

Three weeks later, on Juneteenth, a person identifying as Anonymous leaked hundreds of gigabytes of internal police files from more than 200 agencies across the U.S. The hack, labeled #BlueLeaks, contained little information about police misconduct. However, it did reveal that local and federal law-enforcement groups spread poorly researched and exaggerated misinformation to Minnesota police officers during the unrest in May and June, and made efforts to monitor protesters' social-media activity.

I had recently published a book that detailed the tangled origins of Anonymous, and until last month, I'd thought the group had faded away. I was surprised by its reemergence, and wanted to understand how and why it seemed to be coming back, starting with who had made the new video. It didn't take me long to find out.

The video was watermarked, which is uncharacteristic for Anonymous. The mark is blurred out in copies, but appears in the original post in white font: "anonews.co." That URL led me to a news-aggregation site, which brought me to the site's Facebook page, where the first iteration of the video had been posted on May 28. A British company called Midialab Ltd. controlled the page. I wrote to the email listed on the page, and the company's owner replied the same day. This person requested anonymity but was willing to put me in touch with the creator of the video.

Read the rest here:

https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/

International Board of Directors for 2020-2021

Candy Alexander, CISSP CISM (New England/New Hampshire) has been re-elected as the ISSA International President and will be joined by the following newly elected International Board members:

Curtis Campbell
Jimmy Sanders
Michael Rasmussen

Re-elected International Board Members include:

Mary Ann Davidson (Silicon Valley)
Alex Grohmann

Returning Board Officers Include:

Vice President, Deb Peinert
COO/Secretary, ***Shawn Murray***
CFO/Treasurer, Pam Fusco

A Whopping Rise in Healthcare Cyber Incidents

By Staff, Cyware, August 30, 2020

The healthcare sector has been under tremendous pressure with the increase in the number of those afflicted due to the COVID-19 pandemic and cybercriminals have left no stone unturned to take advantage of this situation.

The numbers speak for themselves

- As of August 13, 2020, the Department of Health and Human Services' HIPAA Breach Reporting Tool has recorded 302 major healthcare breaches impacting nearly 8.7 million individuals.
- Magellan Health, one of the Fortune 500 companies, was struck by a ransomware attack in April 2020. In mid-August, Magellan Health confirmed that about 1.7 million individuals have been affected so far by the April cyberattack.

Healthcare sector allures more

It is often the case that medical facilities have a weaker implementation of security measures as compared to other industries such as banking and financial networks, IT, and e-commerce.

- So far, in August, many healthcare organizations like Illinois healthcare system FHN, Premier Health Partners, MedEvolve, Ashley County Medical Center, Nova Scotia Health, Aberdeen Hospital, Valley Regional Healthcare, and Hampshire Hospitals NHS Foundation Trust have suffered data breaches and unauthorized access incidents.
- In July 2020, National Cardiovascular Partners, Quantum imaging, Heartland Counseling Services Inc., and Hapvida became victims of cyberattacks and data breaches.

Threat actors in the field

The sector has witnessed a wide variety of cyberattacks, including phishing campaigns, ransomware attacks, unauthorized data access, and mishandled health record disposals.

- APT29 group had attempted to steal coronavirus related research and intellectual property from healthcare research organizations, universities, researchers, etc. to steal coronavirus related research secrets between May and July.
- Several other malware and threat actors including FritzFrog, Bazar Backdoor, Hakbit, Evil Corp, etc. were found targeting the healthcare sector (along with some other targeted sectors).
- Ransomware like Netwalker (Center for Fertility and Gynecology, Lorien Health Services), Maze ransomware (Regis Healthcare), etc. also created havoc among healthcare organizations.
- Beaumont Health witnessed a phishing attack, when some email accounts have had unauthorized access between January 3, 2020, and January 29, 2020.

Read the rest here:

https://cyware.com/news/a-whopping-rise-in-healthcare-cyber-incidents-944b8191

To the 10th Annual Peak Cyber Symposium Attendees

Thank you for registering to for Peak Cyber!

I hope you are doing well during these challenging times. We are contacting you because

ISSA-COS has decided to take the 10th Annual Peak Cyber Symposium **virtual** this year. Given the current COVID-19 situation, and new guidelines for attendee capacity at the Doubletree Hilton, it became clear that there was really no other choice but to go **virtual.**

Because we are pivoting to a virtual program we need a little more time to get things in order so we are also pushing the event dates out to November The new schedule will be:

- Monday, **November 16th** – Peak Cyber Job Fair
- Tuesday, **November 17th** – Peak Cyber CTF
- Wednesday, **November 18th** – Peak Cyber Speaker Sessions and Virtual Exhibits
- Thursday, **November 19th** – Peak Cyber Speaker Sessions and Virtual Exhibits

Detailed instructions will be emailed out to you on how to access Peak Cyber via the Whova Event App as the event approaches.

In the meantime, help us spread the word to your co-workers and colleagues. The virtual event will remain ***FREE to attend for all ISSA Members and those with a mil, .gov, or .edu email address.***

COVID-19 has created an extremely challenging business environment, and in the conference industry, it has been even more challenging. We appreciate your understanding and support.

Please feel free to contact me with questions or concerns.

Respectfully,

Dennis O'Neill

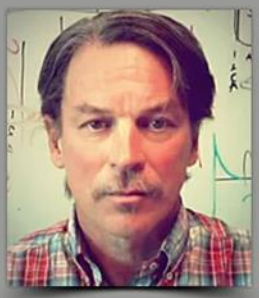
ISSA-COS Peak Cyber Lead

dennis@ssewest.com

Peak Cyber Symposium

KEYNOTE SPEAKERS

Dr. Jim Crowder
Systems Fellow,
Mad Scientist
Colorado Engineering, Inc.



Dr. Rory Lewis
Program Director: Masters of Computer Science, UCCS |
Director: Artificial Intelligence
USAF/A2 WEdge SOCOM

JUST CONFIRMED!

Dr. Dale W. Meyerrose
Major General, U.S. Air Force retired
President, MeyerRose Group

JUST CONFIRMED!

Dr. Kelley Misata
CEO
Sightline Security |
President and Executive Director
OISF (Suricata)

Nathan Toups
Senior Site Reliability Engineer
Santé Capital
Quantitative Hedge Fund

JUST CONFIRMED!

Karen Worstell
CEO
W Risk Group

Early Bird Registration is now open.
Free registration for all ISSA Members, .mil, .gov. and .edu!

www.peakcyberco.com

National Insider Threat Awareness Month

Original release date: August 31, 2020 | Last revised: September 1, 2020

September is National Insider Threat Awareness Month (NIATM), which is a collaborative effort between the National Counterintelligence and Security Center (NCSC), National Insider Threat Task Force (NITTF), Office of the Under Secretary of Defense Intelligence and Security (USD(I&S)), Department of Homeland Security (DHS), and Defense Counterintelligence and Security Agency (DCSA) to emphasize the importance of detecting, deterring, and reporting insider threats.

NITAM 2020 will focus on "Resilience" by promoting personal and organizational resilience to mitigate risks posed by insider threats. The Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to read NCSC's NITAM 2020 endorsement and explore the following resources to learn how to protect against insider threats:

Insider Threat Mitigation
CISA Webinar: A Holistic Approach to Mitigating Insider Threats
NITTF Resource Library
Center for Development of Security Excellence: Insider Threat Awareness and Training

September is National Preparedness Month

Original release date: September 03, 2020 | Last revised: September 09, 2020

September is National Preparedness Month, which promotes family and community disaster planning. This year's theme is "Disasters Don't Wait. Make Your Plan Today." The Cybersecurity and Infrastructure Security Agency (CISA) recommends users and administrators use this month as an opportunity to assess cybersecurity preparedness for cyber-related events, such as identity theft, ransomware infection, or a data breach.

Learn more about preparing for a natural disaster or general emergency at Ready.gov/September. See Ready.gov/Cybersecurity and the following CISA Tips for resources on preparing for, and responding to, unexpected cyber-related events:

- Protecting Against Ransomware
- Avoiding Social Engineering and Phishing Attacks
- Preventing and Responding to Identity Theft
- Protecting Against Malicious Code

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.

Jacobs

ISSA
Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org

ISSA-COS WELCOMES **JACOBS** AS OUR NEWEST ANNUAL CHAPTER SPONSOR!

THANK YOU, JACOBS FOR SUPPORTING OUR CHAPTER, OUR MEMBERS, AND OUR COMMUNITY!

BRONZE

ANNUAL CHAPTER SPONSOR

BeyondTrust

ISSA
Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org

ISSA-COS WELCOMES **BEYONDTRUST** AS OUR NEWEST ANNUAL CHAPTER SPONSOR!

THANK YOU, BEYONDTRUST FOR SUPPORTING OUR CHAPTER, OUR MEMBERS, AND OUR COMMUNITY!

BRONZE

ANNUAL CHAPTER SPONSOR

CLEARED CAREERS

ISSA
Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org

ISSA-COS WELCOMES **CLEARED CAREERS** AS OUR NEWEST STRATEGIC PARNER!

THANK YOU, CLEARED CAREERS FOR SUPPORTING OUR CHAPTER AND OUR COMMUNITY!

CLEARED CAREERS

STRATEGIC PARTNER

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

ISSA
Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org

ISSA-COS SALUTES **MURRAY SECURITY SERVICES (MSS)** AS A RETURNING ANNUAL CHAPTER SPONSOR!

THANK YOU, MSS FOR SUPPORTING OUR CHAPTER, OUR MEMBERS, AND OUR COMMUNITY!

PLATINUM

ANNUAL CHAPTER SPONSOR

SPECIAL INTEREST GROUPS (SIGS)

SIG Overview

The ISSA-COS Special Interest Groups (SIGs) are comprised of Cybersecurity professionals who gather to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: **Affinity Groups** and **Industry Groups**. Through our online forum, ISSA-COS enables our members and the community at large to participant in thoughtfully organized and well-structured categories of conversation. Forum participants can engage in any one of eight different SIGs. Within our forum, we commission Subject Matter Experts who add increased technical knowledge to all the conversational threads.

To maintain positive behaviors within the forum, ISSA-COS has assigned a SIG Program Coordinator who monitors each SIG conversation. The SIG Program Coordinator also monitors the size and degree of participation within each SIG. Once participation reaches a sizable amount, the SIG Program Coordinator will suggest and help organize in-person meet ups. This provides SIG participants an opportunity to put virtual names with physical faces to further strengthen the bonds of interaction taking place in the virtual environment.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups 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 (WIS)
- Young Professional in Security (YIS)
- Educators in Security (EduIS)
- Executives in Security (ExecIS)

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups 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 (FIS)
- Healthcare in Security (HIS)
- Retail in Security (RIS)
- DoD in Security (DodIS)

Technical Approaches to Uncovering and Remediating Malicious Activity

By Staff, CISA, September 1, 2020

Summary

This joint advisory is the result of a collaborative research effort by the cybersecurity authorities of five nations: Australia, Canada, New Zealand, the United Kingdom, and the United States. It highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices. The purpose of this report is to enhance incident response among partners and network administrators along with serving as a playbook for incident investigation.

Key Takeaways

When addressing potential incidents and applying best practice incident response procedures:

- First, collect and remove for further analysis:
- Relevant artifacts,
- Logs, and
- Data.
- Next, implement mitigation steps that avoid tipping off the adversary that their presence in the network has been discovered.
- Finally, consider soliciting incident response support from a third-party IT security organization to:
- Provide subject matter expertise and technical support to the incident response,
- Ensure that the actor is eradicated from the network, and

Avoid residual issues that could result in follow-up compromises once the incident is closed.

Technical Details

The incident response process requires a variety of technical approaches to uncover malicious activity. Incident responders should consider the following activities.

- **Indicators of Compromise (IOC) Search** – Collect known-bad indicators of compromise from a broad variety of sources, and search for those indicators in network and host artifacts. Assess results for further indications of malicious activity to eliminate false positives.
- **Frequency Analysis** – Leverage large datasets to calculate normal traffic patterns in both network and host systems. Use these predictive algorithms to identify activity that is inconsistent with normal patterns. Variables often considered include timing, source location, destination location, port utilization, protocol adherence, file location, integrity via hash, file size, naming convention, and other attributes.
- **Pattern Analysis** – Analyze data to identify repeating patterns that are indicative of either automated mechanisms (e.g., malware, scripts) or routine human threat actor activity. Filter out the data containing normal activity and evaluate the remaining data to identify suspicious or malicious activity.
- **Anomaly Detection** – Conduct an analyst review (based on the team's knowledge of, and experience with, system administration) of collected artifacts to identify errors. Review unique values for various datasets and research associated data, where appropriate, to find anomalous activity that could be indicative of threat actor activity.

Recommended Artifact and Information Collection

When hunting and/or investigating a network, it is important to review a broad variety of artifacts to identify any suspicious activity that may be related to the incident. Consider collecting and reviewing the following artifacts throughout the investigation.

Read the rest here:

https://us-cert.cisa.gov/ncas/alerts/aa20-245a

Is the electric grid closer to a devastating cyberattack that could mean lights out?

By Larry Jaffee, SC Media, August 26, 2020

The Navy took some risk in permitting hundreds of thousands of service members and civilian employees to use personal laptops and cell phones at home during the COVID-19 pandemic to transact normal business, the service's top cybersecurity official said.

Could the electric grid really be taken down with a $50 device secreted in the bottom of a coffee cup as some researchers have claimed? Perhaps. But the more likely threat comes from bad actors with markedly improved capabilities who've ramped up their attacks on critical infrastructure and utilities.

Consider that 70 percent of industrial controls system (ICS) vulnerabilities disclosed in the first half of 2020 can be exploited remotely, according to a report from Claroty, a problem that has grown more acute since the pandemic forced ICS-driven facilities to rely even more on work-from-home personnel, leaving networks further susceptible to unauthorized tampering.

Claroty said the energy, critical manufacturing, and water and wastewater infrastructure sectors were by far the most impacted during the first half 2020 based on the analysis of 363 ICS vulnerabilities published in the National Vulnerability Database (NVD) and 139 ICS advisories affecting 53 vendors issued by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Compared with the first half of 2019, ICS vulnerabilities reported by NVD increased by 10.3 percent from 331, while ICS-CERT advisories increased by 32.4 percent from 105. More than 75 percent of vulnerabilities were assigned high or critical Common Vulnerability Scoring System (CVSS) scores.

Claroty claimed its latest operational technology (OT) data suggests fully air-gapped ICS networks that are isolated from cyber threats have become vastly uncommon, noting remote code execution (RCE) accounted for 49 percent of vulnerabilities. Of the 385 unique Common Vulnerabilities and Exposures (CVEs) included in the advisories, energy had 236, critical manufacturing had 197, and water & wastewater had 171. Compared to the first half of 2019, water and wastewater experienced the largest increase of CVEs (122.1 percent), while critical manufacturing increased by 87.3 percent and energy by 58.9 percent.

Security experts tell SC that the threat to the grid is real, not only orchestrated by nation-states, such as documented attacks in the past decade on power plants in Iran, Saudi Arabia and the Ukraine, but other parties could also cause a potential blackout for an extended period.

"Previously, the threat was always perceived to be nation-state interference," said Mark Kedgley, CTO at New Net Technologies (NNT). "However, we have seen recently with the EKANS/Snake ransomware reports that critical infrastructure now appears to be a target for the organized-crime end of the hacker spectrum." Being able to cut off utilities for a population of several hundred thousand citizens, he added, is a pretty strong hand in a ransom negotiation.

Not all critical infrastructure attacks aim to take the grid down or darken a city, agreed Eran Fine, CEO of NanoLock Security. "With financial attacks, bankrupting a utility or creating lack of trust can also create harm," Fine said. Indeed, a June 2020 research report conducted by Northeast Group reported electricity theft and fraud total $96 billion per year globally.

Utilities' "smart meters" are especially vulnerable to attack, which could erode the trust of its customers, Sjoerd Hulzinga, IoT security product manager for KPN Security, pointed out.

Read the rest here:

https://www.scmagazine.com/home/security-news/is-the-electric-grid-closer-to-a-devastating-cyberattack-that-could-mean-lights-out/

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**

The Pandemic is Pushing the Pentagon Toward *Classified* Telework

By Frank Konkel, NextGov, August 19, 2020

Almost since the department's inception, Homeland Security has been focused on identifying and preventing agency employees with security clearances from becoming insider threats by leaking information, intentionally or otherwise. Now, the department's Insider Threat Program is expanding to include anyone—past or present—who has had any kind of access to agency information.

Since the coronavirus reached pandemic status in March, the vast majority of remote work being performed by Defense Department employees is on the unclassified side. But the lingering pandemic is pushing the Pentagon and its agencies to launch various classified telework pilots that could forever change the way the department operates.

As of August, the Defense Department has expanded its remote work capabilities tenfold to approximately 1 million personnel through its Commercial Virtual Remote collaboration environment, which facilitates the exchange of low-risk, unclassified data and communications among users. The move to facilitating the exchange of classified information remotely among users, however, represents a giant step for the risk-averse Pentagon. Yet it's already happening in some pockets across the Defense Department.

"In the secret and top secret realm, we have kind of cracked how to do telework in that way," Lauren Knausenberger, chief transformation officer at the U.S. Air Force, said during an event hosted by *Nextgov* in early August. "It's just that doing that at scale ... What does that scale mean? It's not really a technical problem as much as it's a, 'Let's make decisions and provision.'"

For decades, the Pentagon's classified work—the handling of data designated at secret, top secret and other classification levels—has been done in physical facilities called SCIFs, or sensitive compartmented information facilities that provide physical barriers to ensure classified data is safeguarded. Increasingly, pilots across the Defense Department are looking for software to provide the same kinds of barriers in the digital realm, according to Stephen Wallace, systems innovation scientist within the Defense Information Systems Agency's Emerging Technology Directorate.

"There's generally more acceptance ... of software-oriented separation," Wallace said, also speaking at *Nextgov*'s August 5 event. "Those kinds of things may drive some commoditization in that space where we're using attributes about data or people or those kinds of things to help create separation versus physically having different stacks of equipment."

Wallace said his team had been prototyping a classified remote Windows capability early in the COVID-19 crisis. The project was elevated from prototyping to "productizing," he said, as the pandemic grew worse.

"Since then, we've put a tremendous more amount of capability out there with respect to how to deal with classified missions, both on premise and off," Wallace said. "I'm pretty excited about where that's gone."

The pilots for classified remote work at the Air Force and DISA, which is the Pentagon's IT arm, are among several others undergoing evaluations at Defense agencies in the coming months.

Read the rest here:

https://www.nextgov.com/it-modernization/2020/08/pandemic-pushing-pentagon-toward-classified-telework/167824/

Most security pros are concerned about human error exposing cloud data

By Mark Rockwell, HelpNet Security, July 13, 2020

A number of organizations face shortcomings in monitoring and securing their cloud environments, according to a Tripwire survey of 310 security professionals.

76% of security professionals state they have difficulty maintaining security configurations in the cloud, and 37% said their risk management capabilities in the cloud are worse compared with other parts of their environment. 93% are concerned about human error accidentally exposing their cloud data.

Few orgs assessing overall cloud security posture in real time

Attackers are known to run automated searches to find sensitive data exposed in the cloud, making it critical for organizations to monitor their cloud security posture on a recurring basis and fix issues immediately.

However, the report found that only 21% of organizations assess their overall cloud security posture in real time or near real time. While 21% said they conduct weekly evaluations, 58% do so only monthly or less frequently. Despite widespread worry about human errors, 22% still assess their cloud security posture manually.

“Security teams are dealing with much more complex environments, and it can be extremely difficult to stay on top of the growing cloud footprint without having the right strategy and resources in place,” said Tim Erlin, VP of product management and strategy at Tripwire.

“Fortunately, there are well-established frameworks, such as CIS benchmarks, which provide prioritized recommendations for securing the cloud. However, the ongoing work of maintaining proper security controls often goes undone or puts too much strain on resources, leading to human error.”

Most organizations utilize a framework for securing their cloud environments – CIS and NIST being two of the most popular – but only 22% said they are able to maintain continuous cloud security compliance over time.

While 91% of organizations have implemented some level of automated enforcement in the cloud, 92% still want to increase their level of automated enforcement.

Additional survey findings show that automation levels varied across cloud security best practices:

Read the rest here:

https://www.helpnetsecurity.com/2020/08/13/most-security-pros-are-concerned-about-human-error-exposing-cloud-data/?web_view=true

Number of Foreign Companies Within Defense Supply Chain Grew Over Past Decade, Report Says

By Mila Jasper, NextGov, August 17, 2020

Reshoring the defense supply chain may reduce national security risks, but a new report detailing a heavy dependency on goods and services from foreign countries like China shows reshoring may be easier said than done.

Researchers at Govini, a decision science company supporting the defense industry, analyzed data from over 1,000 Defense Department vendors across 100 industries to show how supply chain reliance on products from foreign countries has increased over the past decade. According to the survey, the number of Chinese suppliers in DOD's base increased by a total of 420% since 2010.

For cyber and information technology, two statistics stick out. The share of companies based in foreign nations in the supply chain grew the most in the packaged software and IT services between 2010 and 2019. Companies based in foreign countries made up 3% of the packaged software supplier base in 2010. That number rose to 7% in 2019. The numbers are similar for IT services: Companies based in foreign countries made up 3% of the IT services supplier base in 2010 and 7% in 2019.

Tara Murphy Dougherty, CEO of Govini, told *Nextgov* increasing adoption of IT infrastructure is critical for the Defense Department, particularly as COVID-19 forced the agency's workforce into mass telework. But that means it is imperative DOD addresses supply chain concerns for information and communications technology.

Murphy Dougherty said these two investment areas are only going to continue to grow, which means the department needs to act to clearly define its stance on IT supply chain security.

"What are you doing, other than responding to some of the legislation that we've seen come out of the Hill mandating investigation of this?" she said. "It would be great to see more options."

A key mandate from Congress related to supply chain was supposed to take effect on an interim basis Thursday. Section 889 (a)(1)(b) of the 2019 National Defense Authorization Act bans agencies from contracting with companies that do business with five Chinese firms, including Huawei and ZTE. But according to a *Defense News* report, the Pentagon received a temporary waiver from the Director of National Intelligence pushing back the compliance date until September 30.

Defense Undersecretary for Acquisitions and Sustainment Ellen Lord said at a Professional Services Council webinar Thursday she needs feedback from industry on what's working and what's not when it comes to implementing the rule.

Read the rest here:

https://www.nextgov.com/cybersecurity/2020/08/number-foreign-companies-within-defense-supply-chain-grew-over-past-decade-report-says/167752/

Update Your Profile!

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

Zero Trust Architecture: NIST Publishes SP 800-207

NIST announces the final publication of **Special Publication (SP) 800-207, *Zero Trust Architecture***, which discusses the core logical components that make up a zero trust architecture (ZTA). Zero trust refers to an evolving set of security paradigms that narrows defenses from wide network perimeters to individual or small groups of resources. Its focus on protecting resources rather than network segments is a response to enterprise tends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary. ZTA strategies are already present in current federal cybersecurity policies and programs, though the document includes a gap analysis of areas where more research and standardization are needed to aid agencies in developing and implementing ZTA strategies. Additionally, this document establishes an abstract definition of zero trust and ZTA as well as general deployment models, use cases where ZTA could improve an enterprise's overall IT security posture, and a high-level roadmap to implementing a ZTA approach for an enterprise.

Publication details: https://csrc.nist.gov/publications/detail/sp/800-207/final

US offers $10 million reward for hackers meddling in US elections

By Catalin Cimpanu , ZDNet, August 5, 2020

The US Department of State announced today rewards of up to $10 million for any information leading to the identification of any person who works with or for a foreign government for the purpose of interfering with US elections through "illegal cyber activities."

This includes attacks against US election officials, US election infrastructure, voting machines, but also candidates and their staff.

The announcement was made today, less than 100 days until the 2020 US Presidential Election that will have incumbent Donald Trump face off against Democrat candidate Joe Biden.

Nevertheless, the Department of State said the reward is valid for any form of election hacking, at any level, such as elections held at the federal, state, or local level as well.

"Foreign adversaries could employ malicious cyber operations targeting election infrastructure, including voter registration databases and voting machines, to impair an election in the United States," the State Department said today, describing the attacks it fears and wants to stop.

"Such adversaries could also conduct malicious cyber operations against U.S. political organizations or campaigns to steal confidential information and then leak that information as part of influence operations to undermine political organizations or candidates."

The intent is to catch and prosecute any foreign state-sponsored hackers, the Department of State said, describing the ability of foreign state-sponsored hackers to meddle in US elections "an unusual and extraordinary threat to the national security and foreign policy of the United States."

Read the rest here:

https://www.zdnet.com/article/us-offers-10-million-reward-for-hackers-meddling-in-us-elections/

ISSA Information Systems Security Association
Colorado Springs Chapter

WWW.ISSA-COS.ORG

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

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

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: **Vacant**

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
Mentorship Committee Chair: **Vacant**
Media/Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

**** Executive Board Members***

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

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 an East Texas school bullied a cyber attack

By John Anderson, Tyler Morning telegraph, July 31, 2020

It's happened to most of us, or someone we know. An email gets hacked, or a Facebook account and even a debit card connected to a bank account or credit card.

We've heard of companies being hacked as someone opened an email and clicked a link that caused a virus to enter the network, or someone connects to a server from the outside.

This week, it was a school in East Texas, and the results were as good as any crime show on television.

Read the rest here:

https://tylerpaper.com/news/local/column-how-an-east-texas-school-bullied-a-cyber-attack/article_063c082e-d38b-11ea-b9f6-fb512cff9c2d.html

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