Dear Chapter Members,

It’s been a challenging year, and the next two months are your opportunity to chart the course of the chapter. It’s time for board elections for open positions and for you to vote on proposed changes to our chapter bylaws. You will receive emails on both the chapter bylaws and the board candidates.

If you’ve been reading the local papers such as The Gazette and the Colorado Springs Business Journal, you’ve seen the growing number of articles on cybersecurity. Much of this interest is a result of both the National Cybersecurity Center (see Page 8 in this newsletter) and the growing number of high profile attacks. I see these changes as an opportunity to increase the visibility of our chapter and our members. We have hundreds of members that are experts in all areas of cybersecurity – from SCADS and ICS to programming, physical security, server and application security, and networking. I believe this continued interest and growth will be opportunities to exercise and showcase your experience and skills. Your board is working hard to develop relationships with local business and community leaders to create these opportunities.

We need your help. There are going to be more and more opportunities for you to volunteer your skills, knowledge, and training in ways that can benefit you professionally, your chapter, and your (Continued on page 3)

The ISSA Colorado Springs Newsletter incorporates open source news articles as a training method to educate readers on security matters in compliance with USC Title 17, Section 107, Paragraph a.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
Sending Passwords Through Your Body Could Be More Secure Than Transmitting Them Over The Air

By Amy Nordrum, IEEE Spectrum, October 5, 2016

Another day, another cybersecurity threat to worry about. Earlier this week, Johnson and Johnson told patients that it had discovered a security flaw in its insulin pumps, which left the pumps vulnerable to hacking—though the company said the risk of such a hack actually occurring is “extremely low.”

Meanwhile, a group of researchers at the University of Washington in Seattle is offering an alternative to wireless data transmission that could make medical devices and wearables more secure: transmitting the data through our bodies rather than broadcasting them over the air. Their premise is that it’s much harder to surveil a human body without someone noticing than it is to surreptitiously pluck a password from wireless signals in the air.

In tests with 10 subjects, the group showed that it’s possible to transmit passwords at speeds of up to 50 bits per second (bps) through the human body, using off-the-shelf products such as fingerprint scanners and iPhone fingerprint sensors. For comparison, a standard Internet package in the U.S. offers download speeds of 15 megabits-per-second, or 15 million bits per second.

“You can hold a phone in your hand and you can have a receiver on your leg, and you can actually receive signals very strongly,” says Shyamnath Gollakota, a wireless researcher at the University of Washington and collaborator on the project.

The experiments were led by graduate students Mehrdad Hessar and Vikram Iyer with the guidance of Gollakota. The group recently presented its work at the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing in Germany.

If the technique were ever to catch on, it would be limited to applications such as wearables, medical implants, and digital door locks because it requires users to simultaneously touch both the device that is sending the password and the one that is receiving it.

And the low bit rate means it would work best for transferring short strings of numbers such as a passcode rather than full sentences, or high-definition films. As an example, the group says sending a four-digit numerical code to a digital door lock would require fewer than 16 bits, which could be transmitted through the body in less than a second. A 256-bit serial number could be sent to a medical device in under 15 seconds.

Jeffrey Walling, an assistant professor at the University of Utah who has studied capacitive touch, says even this method of on-body password transferral wouldn’t be hackproof. “Certainly, any time you’re transmitting any type of signal, you can’t make it 100 percent secure,” he says. But it could be an improvement over the wireless channels used today.

In the past, other researchers have successfully demonstrated on-body communications but those projects often required users to add custom hardware onto their devices in order to pull it off. To see whether it was possible to do this with existing technology, the University of Washington group selected several commercial devices to test: an iPhone 5s; an iPhone 6s; a Lenovo touchpad; an Adafruit touchpad; and a Verifi P5100 fingerprint scanner.

Read the rest here: http://spectrum.ieee.org/tech-talk/telecom/security/sending-passwords-through-your-body-could-be-more-secure-than-over-the-air
I (and several other folks) will miss the 2 November meeting because we’ll be in Dallas for the ISSA International Conference. I will be presenting the ISSA-COS portion of the Freemium Status Briefing at the Chapter Leaders’ Summit as part of the conference. The Baltimore Chapter will present their perspective on the Freemium Program. The briefing is intended to provide the International Board and attending Chapters with some general perspectives and high level overview of the program. I will provide an update in the December newsletter. As part of the follow on activities from the briefing, we will be working with Baltimore to document our metrics for an International Board decision regarding next steps for the Freemium Program. If you are a Freemium student and have not contacted me regarding the activities you have participated in as well as your perspective on those activities, please do so as soon as possible. I am still collecting and finalizing metrics for our written report. If you have not participated in any of our events, I need to capture that information, too. I would also like to know if the events were relevant and useful (or not)? Any ideas to improve our activities would also be welcome. Your inputs will be critical to our ability to “sell” the Freemium program to the ISSA International board and continue the program. The easiest way would be a quick email to me at dreed54321@comcast.net.

We still need more mentors! We have more people who want mentoring than we have mentors to support the program. Please contact Melissa Absher or me if you can support this worthwhile program for the chapter. It’s a good block to have on your resume when you submit your application for Senior Member, Fellow, or Distinguished Fellow.

We are continuing to increase our membership—up to ~469 members as of October 27th. Overall, we are successfully increasing our membership with renewals and new memberships—both general and students/Freemiums. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in, particularly as the new school year starts! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

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

David Reed
Membership Committee Chairman
dreed54321@comcast.net

(Continued from page 1)

community. These opportunities may only take a few hours once or twice a year – opportunities such as presenting at a Saturday mini-seminar, or helping to man our chapter booth at an event nearby. We also have a need for mentors as well as instructors for our CISSP and Security+ review sessions. Opportunities such as these allow you to broaden your professional experience and may help you become an ISSA Fellow or even Senior Fellow.

Finally, our December awards banquet is around the corner. When you receive your invitation, please respond quickly so that we can plan appropriately. I look forward to seeing you there!

Yours,

Frank
Mini-Seminars

Mini-seminars are designed to provide members an opportunity to learn something new, and earn a few CPE/CEUs, at no cost. Are you missing out on a great opportunity for FREE continuing education credits? Are you missing out on an opportunity to share your knowledge/experience with your fellow Chapter members? Come to our mini-seminars and collaborate with your colleagues!

Mini-Seminar: 5 Nov, 9am-Noon at College America:

Our final mini-seminar for 2016 will be on 5 Nov 9am to noon, at College America (2020 North Academy Blvd). Please note the location for the November mini-seminar. College America has graciously offered us the use of their facility and classrooms for our seminars. We now have two locations, Colorado Technical University and College America, expanding our training options. We thank College America for reaching out to us, and look forward to a new and enduring partnership with them.

Root9B has graciously offered to present at this mini-seminar. From the Root9B website: “Root9B’s executive team and advisory board members are proven leaders in the areas of cyber security, national security, and risk mitigation. We are information security veterans, who over the course of many years have dealt with diverse types of sophisticated cyber adversaries and technical vulnerabilities. We’re trailblazers, breaking new ground with our unique approach focused on active adversary pursuit and tailored cyber operations. Root9B’s leadership and technical teams are comprised of cybersecurity professionals who honed their craft securing DoD networks and communications. Along the way, they battled the same adversaries who represent the biggest threat to businesses and government agencies today—advanced, sophisticated nation-state cyber actors. This experience enables us to think like the adversary.” Come out and hear their presentation on Proactive Response Cybersecurity!

Topics to be covered during this mini-seminar are:

Proactive Response Cybersecurity, Presented by: Keith Smith, Root9B

Intro to Cryptography: “Introduction to Cryptography” provides both an introduction and a refresher on the sometimes strange and wonderful world of cryptography. Learn about the role of crypto in the Kama Sutra, how advances in cryptanalysis changed the outcomes of wars, and the strange and uncertain world of quantum cryptography. Presented by: Mark Heinrich, CISSP

SANS Courses in Colorado Springs

SANS is coming to Colorado Springs! We’ve been working with SANS, trying to get them to bring their courses to Colorado Springs, in addition to Denver. SANS currently has the following courses scheduled on different dates, different locations in the Springs, with discussions ongoing for future courses.

NOTE: ISSA members receive an additional 5% discount on the advertised price. Email the Training Team leads at Training@ISSA-COS.org to get the discount code. Register quickly, these courses may fill up soon!


SEC504: Hacker Tools, Techniques, Exploits and Incident Handling – December 5-10 - https://www.sans.org/community/event/sec504-colorado-springs-05dec2016-staff

Continuing Education (CEU/CPE) Ideas

Do you know there are numerous free or low cost CEU and CPE options available? Check out the ISSA-COS web page (http://www.issa-cos.org/), Training Classes, “On-Line Training” link for suggested sites.

(Continued on page 5)
志愿机会

寻找一个志愿者机会？寻找一种方式来分享你的知识/专长？寻找一种方式来赚取CompTIA CEUs或(ISC)2 CPEs？我们总是在寻找成员来教授安全+或CISSP域。我们提供幻灯片，但你可以根据需要进行修改，只要你的修改与CompTIA或(ISC)2的官方标准保持一致。如果你愿意作为志愿者教授安全+或CISSP域，或者你有疑问，请联系我们的培训委员会领导：Training@issa-cos.org。

如果有你想要我们安排的迷你研讨会的话题，请让我们知道，我们会看看是否有章员愿意为它制作演示文稿。

如果有想法/建议/请求关于培训倡议，请通过email联系我们Training委员会领导：Training@issa-cos.org。

ISSA名标签

你是否想要一个ISSA名标签来佩戴会议、会议和活动？你现在可以直接从这里购买/领取你的名标签：

Blue Ribbon Trophies & Awards
245 E Taylor St (behind Johnny’s Navajo Hogan on North Nevada)
Colorado Springs
(719) 260-9911

虽然他们官方的营业时间是从周一到周五下午5:30，但他们偶尔会在周六营业。这是一个小企业，所以现金/支票会更受欢迎。通过wbusovsky@aol.com发送email来订购。

（上页继续）
China’s 2,000-km Quantum Link Is Almost Complete

By Rachel Courtland, IEEE Spectrum, October 26, 2016

By the end of this year, a team led by researchers from the University of Science and Technology of China, in Hefei, aims to put the finishing touches on a 2,000-kilometer-long fiber-optic link that will wind its way from Beijing in the north to the coastal city of Shanghai.

What will distinguish this particular stretch of fiber from myriad other long-distance links is its intended application: the exchange of quantum keys for secure communication—a sophisticated gambit to protect data from present and future hackers. If all goes according to plan, this Beijing–Shanghai line will connect quantum networks in four cities. And this large-scale terrestrial effort now has a partner in space: A quantum science satellite was launched in August with a research mission that includes testing the distribution of keys well beyond the country’s borders.

With these developments, China is poised to vastly extend the reach of quantum key distribution (QKD), an approach for creating shared cryptographic keys—sequences of random bits—that can be used to encrypt and decrypt data. Thanks to the fundamental nature of quantum mechanics, QKD has the distinction of being, in principle, unhackable. A malicious party that attempts to eavesdrop on a quantum transmission won’t be able to do so without creating detectable errors.

QKD has already made its way into the real world. In 2007, the scheme was used to secure the transmission of votes in a Swiss election. Several years ago, the U.S.-based firm Battelle began to use the approach to exchange information securely over kilometers of fiber between its corporate headquarters in Columbus, Ohio, and a production facility in Dublin, Ohio.

But despite great progress, there has been a stumbling block to wide distribution. “The problem we’ve got is distance,” says Tim Spiller, director of the United Kingdom’s Quantum Communications Hub, a nationally funded project that is building and connecting quantum networks in Bristol and Cambridge, in England.

The challenge is that QKD encodes information in the states of individual photons. And those photons can’t travel indefinitely in fiber or through the air; the longer the distance, the greater the chance they will be absorbed or scattered.

This characteristic has a direct impact on how quickly a quantum key can be generated, explains physicist Jian-Wei Pan, who leads the Chinese projects. If researchers attempted to send signals directly down 1,000 kilometers of fiber, Pan says, “even using all the best technology, we would only manage to send 1 bit of secure key over 300 years.”

Instead, QKD fiber links must have a way to refresh the signal every 100 km or so to maintain a reasonable bit rate. But this can’t be done with conventional telecommunications equipment. The same rules that protect quantum transmission against eavesdropping also prohibit a quantum key from being copied without corrupting it. The solution has been to concatenate, creating a daisy chain of individual quantum links connected by physically secured spots, or “trusted nodes.” Each intermediate node measures the key and then transmits it with fresh photons to the next node in the chain.

The Beijing–Shanghai line will use 32 trusted nodes to create the 2,000-km line. This approach isn’t ideal for security. Because each trusted node has to convert the quantum key back into classical (nonquantum) information before passing it on, an eavesdropper at the node could potentially hack the data stream there undetected. “That’s the drawback,” Pan says. But the approach is “still much better than traditional communications... [where] there is the possibility of performing eavesdropping” at every point along the route, he says. Here, the problem is limited to 32 spots under lock and key.

“A long-distance chain link like this, [it’s] really the first time it’s been done,” says Grégoire Ribordy of ID Quantique, based in Geneva, which makes hardware for QKD networks. “It’s inspiring other people to try to do similar things around the world.”

If you want to avoid even the small vulnerability of trusted nodes, Spiller says, long-distance QKD must use quantum entanglement, a property that can link the states of photons separated by great physical distance and that can be exchanged between photons. “Quantum repeaters,” used in place of trusted nodes, could take advantage of this phenomenon to relay a quantum key without having to measure it. But this technology is still in an early stage of development, says Spiller; among other things, a quantum repeater will likely require a form of quantum memory to help coordinate communication.

Read the rest here:
Understanding IoT botnets

By Marc Laliberte, HelpNet Security, October 28, 2016

If you were online on Friday October 21st, you were probably affected by the DDoS attack against managed DNS provider Dyn.

Dyn observed that tens of millions of IP addresses participating in the attack were from IoT devices infected by the Mirai botnet. But what exactly is an IoT botnet? What was so different about this DDoS attack and why does it have security professionals so worried?

A botnet is a collection of connected devices which have been infected with malware that allows an attacker to gain remote control and coordinate their actions. Attackers most commonly use their botnets to launch DDoS attacks, but they can also be used to send spam emails, sniff out sensitive passwords, or spread ransomware.

Botnets are created when a victim’s computer or Internet-connected device is infected with a botnet virus or worm. Some botnets are able to self-propagate, finding and infecting vulnerable hosts automatically. Other botnets require a user to unknowingly infect their own computer by installing malware.

IoT offers a new avenue of attack

The rapid proliferation of IoT devices and their lack of security opens up a brand new avenue for botnet creators, and we are now starting to experience the resulting impact. The Mirai botnet that took down Dyn is believed to be created with the same malware that launched two record-setting DDoS attacks in September against the KrebsonSecurity.com and French webhost OVH.

The Mirai botnet follows the same formula of most botnet malware by performing two main functions; growing the botnet by finding and infecting more vulnerable hosts, and launch DDoS attacks using the infected hosts. Where Mirai and other IoT botnets differ from traditional Windows-based botnets though is their devastating effectiveness in spreading to a huge number of IoT device hosts.

In comparison to traditional Windows-based botnets, IoT botnets flourish thanks to a lack of security by design with most IoT devices. Many IoT manufacturers don’t have experience securing network connected devices and often opt for off-the-shelf, embedded operating systems without default settings and exposed network services.

To cap it off, the simplistic designs and functions of most IoT devices lead to users configuring them with the default or easily guessed passwords, leaving them wide open to brute-force takeovers by attackers. When consumers connect these IoT devices directly to the internet (an unfortunately common practice with IoT security cameras for example) they become exposed to every vulnerability and botnet scanner in use.

To make matters worse, it’s very difficult to tell when an IoT device had been infected with botnet malware. With personal computers, the user can typically discover a malware infection through normal use when the machine begins behaving erratically or issues with host-based antivirus detection start to crop up. But users usually interact with IoT devices through a limited web-based GUI rather than accessing the embedded OS, so this lack of interaction allows botnet infections to go unnoticed for extended periods of time.

How Mirai works

The creator of the Mirai botnet recently released the source code for command and control server and the botnet client itself, allowing us a look into exactly how this malware functions. When a host becomes infected by Mirai, the malware starts by killing all other competing malware infections on the device, probably to free up resources for more effective attacks from the infected host.

Mirai then uses the infected host to scan for other vulnerable hosts on the internet and attempts to gain access using a brute force dictionary attack of common usernames and passwords. Once it gains access to a vulnerable host, it installs the Mirai malware and adds the new host to the botnet. While self-propagating, Mirai also checks in with a Command and Control server for instructions and then launches DDoS attacks against designated targets.

IoT botnets are here to stay

Attackers will likely invest more resources into taking over the hordes of IoT devices added to the Internet every day. Industrial IoT device manufacturers need to use the recent attacks as a wakeup call to refocus on securing their products. At a minimum, manufacturers should remove unnecessary network services and include ways to easily or automatically patch security vulnerabilities in their products.

IoT consumers should treat their devices similarly to their personal computers when it comes to security best practices. Here are a few simple steps you can take to make your new smartwatch or connected home gadget more secure:

Read the rest here: https://www.helpnetsecurity.com/2016/10/28/understanding-iot-botnets/
National Cyber Center takes shape


In the past month, the National Cybersecurity Center has solidified its plans — hiring a new CEO, developing a logo and preparing for its first event at The Broadmoor to educate elected officials about cybersecurity.

But as CEO Ed Rios told city and business leaders during a community update Oct. 20, while staff will most likely move into the center’s permanent home at 3650 N. Nevada Ave. next summer, the nonprofit still needs more data, partners, subject matter experts and donations to maintain its current progress.

“There is a lot of expectation and the problem is: We’re a startup,” Rios said. “We need your help in identifying resources. We’re trying to pull together different entities, for-profit and nonprofit, to bring immediate and viable capability to the NCC.”

Initial capability for the NCC will start Tuesday, Nov. 1. Other progress requires a business plan for the center’s three pillars: the Cyber Institute, Rapid Response Center and the Cyber Research, Education and Training Center. Professional services firm PricewaterhouseCoopers is helping the NCC develop its plans.

So far, the NCC has raised nearly $25.9 million from government and private sector donations and grants.

It received $7.8 million from the Colorado Legislature to renovate the former TRW building to house the NCC; $6 million from Congress through UCSS to train Army reservists; $300,000 from philanthropic charitable organizations; $215,000 from private individuals; $35,000 from corporate entities; and $11 million from in-kind contributions, including the UCSS facility. In addition, they’ve requested $550,000 in grants.

Through the winter, JE Dunn Construction will continue renovations at UCSS’s 135,000-square-foot facility, restoring plumbing, heating, ventilation and air conditioning and removing asbestos.

“But the nearly $8 million doesn’t include any build out, [it’s] just for renovations,” Rios said.

NEXT STEPS

To develop capabilities for training, education and research, the NCC is seeking experienced cyber experts and companies in government and the private sector to collaborate — not compete with, said UCSS faculty member Ed Anderson, who served as NCC interim director until earlier this month.

“We intend to be a collaborative organization and are very specific and sensitive to that,” he said.

“We want to make sure public and private partners are a part of the solution.”

Since March, the NCC board of directors and staff have been building the foundation for the organization, speaking to hundreds of professionals and local, state, federal and private organizations to understand the scope of cybersecurity and gaps needing to be addressed.

“We’ve made an aggressive effort to learn what’s going on,” Anderson said.

The Cyber Institute is the most established partner; 50 governors from across the country, as well as state legislatures and county commissioners have been invited to the center’s debut event Nov. 13-15.

“These are leaders responsible for making decisions on key resources and policy, and they don’t know enough about cybersecurity,” Anderson said. “During that time we’ll also be interviewing three board candidates.”

The Rapid Response Center will serve as a 911 center for smaller companies that experience an attack or breach; it will be staffed by volunteers, leading experts in information technology, software and cybersecurity.

“Generally, Fortune 500 companies have all of the resources available to either have their own cybersecurity capability or resources to bring in experts to help if they have a problem,” Anderson said. “The ones who don’t have that capability are the unfortunate 50,000 small- to medium-sized businesses and that is the gap that’s not being adequately addressed. Our intent is to address that issue and work together.”

CHANGING CYBER

Cybersecurity is cultural, generational and always changing, said Rios, and those characteristics will be considered as part of the NCC’s Cyber Research, Education and Training Center.

“We tend to think of cybersecurity in terms of computer engineering, software engineering and computer science, and those are all necessary things,” he said. “But let’s take it a step further and think about including higher education programs in cyber anthropology, sociology and cyber economics, those types of consequences that happen as a result of cyber around the nation.”

And every generation has its own perspective of cyber, Rios said.

Read the rest here:
http://www.csbj.com/2016/10/31/national-cyber-center-takes-shape/
States Move to Protect Their Voting Systems

By Damian Paletta, Wall Street Journal, October 30, 2016

The test began at 8 a.m. last Tuesday. Secretary of State Michele Reagan, four staffers and a freelance Spanish-language interpreter cast 138 votes on 40 ballots using seven touch-screen machines. The mood was jovial—until a printout showed the numbers on one machine didn’t line up with the master list of votes.

Janine Petty, Arizona’s deputy state election director, scanned the printout and quickly discovered another of Ms. Reagan’s staffers had voted for two of the wrong candidates. The machine had worked perfectly, after all.

Ms. Reagan jokingly admonished the sheepish staffer, telling him he should go on their fictional “Wall of Shame.”

Across the country, state election officials are carrying out final tests on tens of thousands of voting machines that are part of a multistep process that delivers results in local, state and federal contests. Next week, the last of more than 120 million ballots are expected to be cast in a watershed election to determine who controls the White House, Congress and the direction of the Supreme Court.

In a span of hours, the votes will be counted in places ranging from the Moose Lodge in Key West, Fla., to a fire hall in Kodiak, Alaska, relayed to state capitals and then broadcast around the world. The process was designed so the federal government didn’t oversee it, but new fears about hackers from abroad have led to a scramble to see if the security protocols in place are sufficient.

In Arizona, officials have been on edge for months. In July, a Russia-linked hacker posted online the stolen login credentials of a Gila County election official, spooking Ms. Reagan and others around the country. They know now that protecting the voting process means guarding against much different threats than they have confronted in the past.

“We’re not dealing with a couple of kids sitting in their bedroom,” she said, sitting on an eight-seat plane on the way to Parker. “It’s cyberwarfare. These little state agencies are not the Pentagon. We don’t have the resources.”

Hackers have scanned the election systems of at least 20 states, U.S. officials said, and now close to 40 states are working with the Department of Homeland Security to try to protect their election systems from digital tampering.

As part of that effort, DHS is running a scan of the internet-linked state election systems to look for vulnerabilities, such as digital doors that hackers might be able to open. Through these reviews DHS officials learned that roughly 20 states had their election systems “scanned” by outside groups in a way that is akin to casing out a site for a future robbery, a DHS official said.

DHS officials also discovered a broad range of computer security tools are used by states, and some needed to have their software updated or put in place new protections. They haven’t yet found any “catastrophic” weaknesses, the DHS official said.

Beyond cyber issues, there are other concerns. Republican presidential nominee Donald Trump has promoted unsubstantiated rumors of vote rigging and fraud, saying illegal immigrants have entered the U.S. from Mexico and will cast millions of votes.

Arizona has dealt with voting challenges for decades, taking pride in its history as a hardscrabble libertarian frontier At one time, it loaded ballots onto mules for a 10-mile trek from a polling site at the base of the Grand Canyon to its rim. But in July, the state had to take the entire voter registration system offline to ensure that the hacker who had stolen the Gila County login credentials hadn’t tampered with the information of 3.4 million voters.

Russian officials have denied trying to interfere in the November elections, but the threat has awakened new fears.

“No one, not even the federal government, can protect themselves against the most sophisticated threat,” said Joseph Lorenzo Hall, an election security expert and chief technologist at the Center for Democracy and Technology. “What you see is people realizing that we have not been attuned to certain threats. Everyone is adopting armor.”

Even though Ms. Reagan and other state officials believe their voting machines cannot be hacked, they worry that antagonists could confuse the public by publishing false results on social media or temporarily knocking a state election site offline.

Read the rest here:

Growth in IT Security Workforce Picks Up
Cybersecurity Employment at Record Levels, But Still Doesn't Meet Demand

By Eric Chabrow, GovInfoSecurity, October 13, 2016

Although an analysis of the latest government statistics confirms continued growth in the information security workforce, the supply of security expertise isn't meeting the demand.

Information Security Media Group’s analysis of the latest quarterly employment numbers from the U.S. Bureau of Labor Statistics shows the size of the information security analysts workforce has soared by 68 percent since the BLS began producing these jobs reports in 2011.

In the third quarter, the number of workers in the United States who consider themselves information security analysts stood at an annualized 88,000, up from 80,500 in the second quarter and 72,800 a year earlier.

Numerous efforts are underway to help boost the security workforce. For example, in the past decade, scores of colleges and universities have introduced information security degree programs. Also, many companies have identified workers, often with programming and other computer expertise, and provided them the training to become information security professionals. Among the best known programs are competitions, such as those sponsored by the U.S. Cyber Challenge, which introduces students and young workers to cybersecurity and allows them to participate in contests that tests their security skills.

"The cyber challenges around the country - and world - are a positive influence on building the workforce," says Elise Yacobellis, manager of the Global Information Security Workforce Survey published by (ISC)², an international, not-for-profit organization that provides IT security education and certification. "They're exposing IT security as a separate profession that could be sought out versus just the IT field. It helps them understand at a hands-on level what they'll possibly be doing if they were to move into this career. And, it also helps them understand if they like it, they have the aptitude for it and this is something they want to pursue."

None of these programs are flooding the job market with IT security specialists, often with programming and other computer expertise, and provided them the training to become information security professionals. Among the best known programs are competitions, such as those sponsored by the U.S. Cyber Challenge, which introduces students and young workers to cybersecurity and allows them to participate in contests that tests their security skills.

"Growth is very shallow and is at risk from the perspective that we clearly don't have a good number of deeply experienced professionals in this field," says Danny Miller, systems CISO at Texas A&M University. "I know of companies that have lots of openings, but no qualified personnel to fill them."

Still, IT security expertise can be found in other computer fields, especially database administrators, network and computer systems administrators, computer systems analysts and computer network architects.

And those occupations also are experiencing growth. Computer occupations have seen a steady climb, with more than 5 million people working or seeking work in a variety of information technology jobs, according to the ISMG analysis. That's a jump of 22 percent - or 4.6 percent annualized - since the BLS implemented its new way to calculate employment at the beginning of decade, according to the ISMG analysis.

Read the rest here:
http://www.govinfosecurity.com/growth-in-security-workforce-picks-up-a-9450?rf=2016-10-13-eg&mtk_tok=eyJpIjoiTVRNMk99UVTFRFkT1dNeSIsIiIsIiI6IiIsInQiOjJRQnU4UDNVAxFja0pPQ14NmZSb25pS0xDUWVvK3FCVUtodXd5U2t3eUZaTmxo0UDhZaG05OXhGSwV2ZoUGY4QR0aG4reGIQVE3UnpSYmJ2KzRBUUs0RVFrNzE3OEFGZGdzNTQ1Rnl0aS1E9ln0%3D

GET A JOB!

Colorado Springs ISSA chapter member Melody Wilson maintains a “Jobs” page at Cyberjoblist.com. There is no charge. The jobs are set to remain listed for 30 days. Job listing originators re-post them again for another 30 days. It is designed for Colorado Springs, but once in awhile a job is listed outside the area.

You can also sign-up on the Cyberjoblist.com site for Job Alerts to be notified when a new job listing is posted!
‘Security Fatigue’ Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests

By Evelyn A Brown, NIST, October 4, 2016

After updating your password for the umpteenth time, have you resorted to using one you know you’ll remember because you’ve used it before? Have you ever given up on an online purchase because you just didn’t feel like creating a new account?

If you have done any of those things, it might be the result of “security fatigue.” It exposes online users to risk and costs businesses money in lost customers.

A new study from the National Institute of Standards and Technology (NIST) found that a majority of the typical computer users they interviewed experienced security fatigue that often leads users to risky computing behavior at work and in their personal lives.

Security fatigue is defined in the study as a weariness or reluctance to deal with computer security. As one of the study’s research subjects said about computer security, “I don’t pay any attention to those things anymore…People get weary from being bombarded by ‘watch out for this or watch out for that.’”

“The finding that the general public is suffering from security fatigue is important because it has implications in the workplace and in people’s everyday life,” cognitive psychologist and co-author Brian Stanton said. “It is critical because so many people bank online, and since health care and other valuable information is being moved to the internet.”

“If people can’t use security, they are not going to, and then we and our nation won’t be secure,” Stanton said.

The study, published this week in IEEE’s IT Professional, draws on data from a qualitative study on computer users’ perception and beliefs about cybersecurity and online privacy. The subjects ranged in age from their 20s to their 60s, hailed from urban, suburban and rural areas, and held a variety of jobs.

The interviews focused on the subjects’ work and home computer use, specifically about online activity, including shopping and banking, computer security, security terminology, and security icons and tools.

“We weren’t even looking for fatigue in our interviews, but we got this overwhelming feeling of weariness throughout all of the data,” computer scientist and co-author Mary Theofanos said.

“Years ago, you had one password to keep up with at work,” she said. “Now people are being asked to remember 25 or 30. We haven’t really thought about cybersecurity expanding and what it has done to people.”

The multidisciplinary team learned that the majority of their average computer users felt overwhelmed and bombarded, and they got tired of being on constant alert, adopting safe behavior, and trying to understand the nuances of online security issues.

When asked to make more computer security decisions than they are able to manage, they experience decision fatigue, which leads to security fatigue.

Researchers found that the result of weariness leads to feelings of resignation and loss of control. These reactions can lead to avoiding decisions, choosing the easiest option among alternatives, making decisions influenced by immediate motivations, behaving impulsively, and failing to follow security rules.

Comments among those who expressed feelings of security fatigue included:

- “I get tired of remembering my username and passwords.”

- “I never remember the PIN numbers, there are too many things for me to remember. It is frustrating to have to remember this useless information.”

- “It also bothers me when I have to go through more additional security measures to access my things, or get locked out of my own account because I forgot as I accidentally typed in my password incorrectly.”

Read the rest here:

Cyber Mission Force approaches initial operating capacity

By Mark Pomerleau, C4ISRnet, October 3, 2016

In a major milestone, U.S. Cyber Command announced that the Cyber Mission Force is nearly initially operationally capable. A CYBERCOM spokesman said, as of Oct. 3, 99 percent of the CMF achieved initial operating capability with 132 of the total 133 teams reaching IOC by the end of fiscal 2016, Sept. 30.

“We set the bar for Initial Operating Capability (IOC) very high, both in terms of our standards and the time available,” Col Daniel J. W. King said. “Building a capability from scratch is an extraordinary challenge and we very nearly met our mark. Thousands of soldiers, sailors, airmen, Marines and Coast Guardsmen answered that call and it is because of them that we continue to strengthen our Cyber Mission Force every day. This has always been about achieving rigorous standards in the shortest time available and I am confident that we will reach IOC very shortly.”

The announcement follows the assertion by CYBERCOM Commander Adm. Michael Rogers in front of the Senate Armed Services Committee last month that the CMF will reach IOC by the end of September, the date long set for IOC.

“The Department of Defense concluded several years ago that defending the nation in cyberspace requires a military capability, operating according to traditional military principles of organization for sustained expertise and accountability at a scale that lets us perform multiple missions simultaneously,” Rogers said in provided written testimony to the committee in April. “When we started to build that capability in early 2013, we had no cyber mission force, no ability to generate or train such an entity and scant ability to respond at scale to defensive requirements or requirements from combatant commanders.”

Cyber Command itself reached full operational capacity (FOC) in 2010. The Cyber Mission Force is expected to reach FOC in 2018.

The 133 teams will comprise of several sub teams with varying roles:

- 13 National Mission Teams that defend the nation.
- 68 cyber protection teams that work to defend DoD networks.
- 27 combat mission teams that provide support to combatant commanders and generate effects in support of operational plans and contingencies.
- 25 support teams that provide analytic and planning support to the national mission teams.

Read the rest here:
http://www.c4ismr.com/articles/cyber-mission-force-reaches-initial-operating-capacity

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
How to Intelligently Share Cyber Threat Intelligence

By Adam Meyer, SecurityWeek, October 28, 2016

A lot has been written on the importance of information sharing in the cybersecurity community. There is seemingly an ISAC for every industry these days. We’re talking the talk, and on the surface it looks like some organizations are starting to walk the walk. But in reality, we’re still just scratching the surface when it comes to sharing cyber threat information, let alone sharing intelligence that is useful and practical.

The concept of intelligence sharing goes way beyond the stream of acronyms such as STIX, TAXII, CybOX, etc. Not to take away from the importance of a standardized format, but that’s just one small piece of the puzzle to make this work - and to get others to give as much as they might take.

Let’s step back for a second and look at why intelligence sharing is important. What’s the benefit and is it worth the effort? At the end of the day, threat intelligence analysts should be working to affect positive change from a cyber risk perspective. Consumers of that intel should be measuring the value of the intelligence, things like: Is the organization safer, and is cybersecurity spend more cost-effective? Practical cyber threat intelligence can absolutely help an organization focus on their most critical risk areas - and sharing can play an important role in all of this.

Before you can start intelligently sharing threat intel, there are several important things you must do first...

Lay the Groundwork

- Establish a collection plan. You can’t really start worrying about what intelligence to share until you first have a collection plan. Your collection plan can include numerous pieces, including your own internal data, open source intelligence, dark web - both open and from restricted sites, commercial data feeds and ISACs. The more sources you can cultivate, the more breadth and depth you have from which to start conducting real intelligence work.

- Identify key stakeholders with whom to share intel and specify who is a producer and who is a consumer. Once you have a collection plan and start collecting data, you also should identify the key stakeholders within your organization as well as within your partners, customers and vendors -- all of whom have digital touchpoints into your organization. Some stakeholder examples include, but are not limited to: executives and boards of directors, technical teams (cybersecurity, IT, application owners), fraud teams, risk management, legal counsel and compliance officers, vendors in your supply chain, and your industry ISAC.

Turning on a spigot of data streaming to your stakeholders isn’t very helpful and in fact can create a lot of ineffective work. This is where the difference between evaluated intelligence and unevaluated data come into play. Your stakeholders should ultimately help determine what data and intelligence gets shared, with emphasis on fulfilling a purpose.

- Of all the data you’ve collected, reviewed and analyzed, what is relevant and does that relevancy change based on who you share it with?

- There should be agreed upon rules of engagement: What types of intelligence do different groups want to see, and what stakeholder data would be most helpful for you?

- What outcomes are you looking to affect change against?

Depending on your organization, there may be more or less stakeholders involved, but the larger point is that cyber threat intelligence has a value to many different roles and organizations. The intelligence you create and share must meet the road against? What data and intelligence gets shared, with emphasis on fulfilling a purpose.

- Incentivize your stakeholders to share. Intelligence sharing only works if everyone is incentivized to share - and if the liability concerns are minimized. Human nature and a highly litigious environment are forces of nature that go against the concept of intelligence sharing. Industry ISACs are great, but the information is typically going to be more general and less personalized to your organization - outside of being from within the same industry.

So taking the concept of the ISAC and making it more tailored to your business ecosystem is where the rubber meets the road - aka creating your private ISAC (more on this below). Your stakeholders, including your suppliers, partners and customers, should all have a stake in this. With all of the interconnectivity amongst you, a threat to one could very well be a threat to the others.

Read the rest here:
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?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!

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

Send your article ideas to Don Creamer at:

doncream-issa@q.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

10 weird and wonderful Wi-Fi names

By Aaron W., Spiceworks, October 10, 2016

When Steve Jobs first demonstrated Wi-Fi with the tangerine-colored iBook in 1999, people cheered and clapped in amazement. That amazement was justified: Wi-Fi was a brand new technology that few people outside of the tech community had seen. As a standard, Wi-Fi was barely two years old.

Nowadays, Wi-Fi is everywhere from the office to the home to the coffee shop to the airport. It's such a common technology that it's become difficult to stand out amongst the sea of wireless network names. And let's be honest: Most people do a really bad job of naming their Wi-Fi networks. DG16508? Linksys9? Please. We can all do better than that.

Read the rest here:


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