Happy Anniversary!

ISSA-COS is 25 Years’ Old!

Colleagues,

The Colorado Springs ISSA chapter has been a chapter for 25 years! At the CSTTF in August we are having a social to talk about the past and the future. This is an ISSA member only event and will be held on 24 August at 5 pm at the DoubleTree by Hilton, Colorado Springs. It will be a chance to socialize with old and new members of the chapter. You should be able to hear stories of the past and ideas for the future. Sign up through EventBrite for the event so we’ll know who will be there.

I have been a member since 2002 and have seen the chapter grow from 10 to 20 people at the luncheons to our current numbers of 80 to 90. When I joined our luncheons were at a BBQ place called Bennett’s. We had a small back room, few sponsors and paid for our own lunch. George Proeller was the President at the time. He believed in the chapter, and what it could be. It grew too big for Bennett’s and was moved to Bambinos. George went on to be an international director and still have connections to the chapter. There we saw Mark Spencer as our president. What a great and hardworking president. He kept the chapter moving forward through rough economic times. He worked hard to get sponsors so members

A Note From Our President

By Ms Cindy Thornburg

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.
The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters

By Bruce Schneier, Motherboard, July 25, 2016

Because users are protected by a veil of technological anonymity, the dark web is often portrayed as a space beyond the reach of law enforcement, where criminals can run amok without fear of prosecution.

Disaster stories involving the Internet of Things are all the rage. They feature cars (both driven and driverless), the power grid, dams, and tunnel ventilation systems. A particularly vivid and realistic one, near-future fiction published last month in New York Magazine, described a cyberattack on New York that involved hacking of cars, the water system, hospitals, elevators, and the power grid. In these stories, thousands of people die. Chaos ensues. While some of these scenarios overhype the mass destruction, the individual risks are all real. And traditional computer and network security isn’t prepared to deal with them.

Classic information security is a triad: confidentiality, integrity, and availability. You’ll see it called “CIA,” which admittedly is confusing in the context of national security. But basically, the three things I can do with your data are steal it (confidentiality), modify it (integrity), or prevent you from getting it (availability).

So far, internet threats have largely been about confidentiality. These can be expensive; one survey estimated that data breaches cost an average of $3.8 million each. They can be embarrassing, as in the theft of celebrity photos from Apple’s iCloud in 2014 or the Ashley Madison breach in 2015. They can be damaging, as when the government of North Korea stole tens of thousands of internal documents from Sony or when hackers stole data about 83 million customer accounts from JP Morgan Chase, both in 2014. They can even affect national security, as in the case of the Office of Personnel Management data breach by—presumptively—China in 2015.

On the Internet of Things, integrity and availability threats are much worse than confidentiality threats. It’s one thing if your smart door lock can be eavesdropped upon to know who is home. It’s another thing entirely if it can be hacked to allow a burglar to open the door—or prevent you from opening your door. A hacker who can deny you control of your car, or take over control, is much more dangerous than one who can eavesdrop on your conversations or track your car’s location.

Today’s threats include hackers crashing airplanes by hacking into computer networks, and remotely disabling cars, either when they’re turned off and parked or while they’re speeding down the highway. We’re worried about manipulated counts from electronic voting machines, frozen water pipes through hacked thermostats, and remote murder through hacked medical devices. The possibilities are pretty literally endless. The Internet of Things will allow for attacks we can’t even imagine.

The increased risks come from three things: software control of systems, interconnections between systems, and automatic or autonomous systems. Let’s look at them in turn:

**Software Control.** The Internet of Things is a result of everything turning into a computer. This gives us enormous power and flexibility, but it brings insecurities with it as well. As more things come under software control, they become vulnerable to all the attacks we’ve seen against computers. But because many of these things are both inexpensive and long-lasting, many of the patch and update systems that work with computers and smartphones won’t work. Right now, the only way to patch most home routers is to throw them away and buy new ones. And the security that comes from replacing your computer and phone every few years won’t work with your refrigerator and thermostat: on the average, you replace the former every 15 years, and the latter approximately never. A recent Princeton survey found 500,000 insecure devices on the Internet. That number is about to explode.

Read the rest here:

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

We are continuing to increase our membership—up to 434 members as of the end of July. We are successfully increasing our membership with renewals and new memberships—both general and students. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

We will continue to push our Freemium student program. We currently have 31 Freemium students as well as several other student members. We will be trying to track participation metrics to support our case for making the Freemium program a permanent program within ISSA. I would personally appreciate hearing from our Freemium students periodically regarding what activities they have participated in as well as their perspective on those activities. Were they relevant and useful? 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 so please take a couple of minutes and provide some feedback to us. The easiest way would be a quick email to me at dreed54321@comcast.net.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

would not have to pay for meals at the meeting. Pat Laverty came on board as president and pushed the chapter even further. Working with other members started the mentorship program with UCCS. Pat also added more position on the board to get more members involved in the chapter.

The chapter has also grown from mostly “grey hair” men to more females and less “grey hair”. It has also grown from just training people for Security+ and CISSP to mini seminars. The chapter has a professional looking website and a big thanks to Bill Welker for all of his hard work. As a chapter, we work together and discuss topics as one, generally having many different views but always being professional.

I hope to see many of you on the 24th.

Cindy
Mini-seminar: 15 Oct, at CTU, 9am-Noon:

Our 25 June and 16 July mini-seminars were a great success, thanks to Russ Weeks, Srikant Mantravadi, Kurt Danis, Wally Magda, and Al Green, and their excellent presentations! These mini-seminars are designed to provide members an opportunity to learn something new, and earn a few CPE/CEUs, at no cost. Our next mini-seminar will be 15 October 9am to noon, at Colorado Technical University (CTU). Topics to be covered during this mini-seminar will be announced later. Please note that there will be no mini-seminars in August or September due to the CISSP Exam Prep Review Seminar held during those months.

The topics listed below have been presented at our mini-seminars. 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!

- Payment Card Industry – Data Security Standard (PCI-DSS): Presented by Art Cooper
- NIST Risk Management Framework (RMF): Presented by Mark Spencer
- Security Architecture: Presented by Bill Blake
- Social Engineering/Phishing: Presented by Debi Caldwell
- Managing IT Security Projects: Presented by Russ Weeks
- Impact of the Internet of Things on Privacy: Presented by Srikant Mantravadi
- Certification Panel & Presentation: Presented by Kurt Danis
- How do we keep the lights on when everyone has access to the switch? Presented by Wally Magda
- Windows 10 Home Edition: It Begins with Securing the Endpoint: Presented by Al Green

The idea of these "mini-seminars" is for members to give a 30 min or 1 hour (or longer) presentation on a topic of interest. Those giving the presentations would earn CPEs/CEUs for the time spent preparing their presentation, and those attending would earn CPEs/CEUs for their attendance and participation in any discussions. If you’re interested in presenting a topic, please email our Training Committee leads at: Training@issa-cos.org and let us know the topic you’d like to present and approximately how much time you’d like for your presentation. If there’s a topic you’d like us to cover during a mini-seminar, please let us know and we’ll see if someone in the Chapter is willing to develop a presentation for it.

This is a great training opportunity for those needing CPE/CEUs to maintain their existing certifications, or anyone wanting to broaden their knowledge. It’s also a great opportunity to share your knowledge and experience with other members of our Chapter, and gain experience as a speaker, by volunteering to be one of our presenters.

Security+ Seminar:

Our March and June Security+ Seminars were very successful, thanks to our volunteer instructors: Frank Gearhart, Cindy Gravely, Derick Lopez, Kurt Danis, and Shawn Murray. No additional Security+ Seminars are currently planned for the rest of the year. If you’re interested in attending a Security+ Seminar, please email our Training Committee leads at: Training@ISSA-COS.org, and let us know. An additional Security+ Seminar may be scheduled, as required, based on emails received.

CISSP Seminar:

This year’s CISSP Seminar started 30 July and will be held on five alternating Saturdays: 30 Jul, 13 & 27 Aug, and 10 & 24 Sep. Do you already hold the CISSP certification? Did you know you can attend the CISSP Seminar for a refresher at no cost and obtain CPEs? This is another great way to maintain your certification, and is an excellent benefit of being a member of ISSA-COS. If interested in attending any of the CISSP Seminar classes, please email the Training Committee leads at: Training@issa-cos.org to ensure we have a seat available for you, and to ensure we have a CPE certificate for you.

(Continued on page 5)
CISSP Study Guides

Did you know that (ISC)² members are able to purchase the CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, 7th Edition for a 50% retail discount? Log into (ISC)², and scroll down to the Security Central section. From there, look for the section that says: (ISC)² Textbook Discounts Get 50% off the Official CBK guides to all (ISC)² certifications. Click on the link provided.

Prefer a different CISSP study guide, or want an additional CISSP study guide? Sybex and Shon Harris both have updated their CISSP study guides, per the 2015 CISSP Common Body of Knowledge (CBK). Both books are now available. Ensure you purchase the 7th edition of either book (updated per the 2015 CBK) to get the latest and most current information.

SANS

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. Based on responses and comments from the survey we did a couple months ago, these courses are what many of you requested. Register quickly, they 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

Physical and Cybersecurity for Critical Infrastructure Training Course

This course will be taught in Colorado Springs on September 29, 2016, and it appears to be free, and provides 8 continuing education units.

The Texas A&M Engineering Extension Service (TEEX) is offering a new course for practitioners managing physical and cybersecurity. The course is the result of a partnership between TEEX, the NPPD Office of Infrastructure Protection and Office of Cybersecurity and Communications, and the FEMA National Training and Education Division. The new course, MGT 452 - Physical and Cybersecurity for Critical Infrastructure, encourages collaborative efforts among individuals and organizations responsible for both physical and cybersecurity toward development of integrated risk management strategies that lead to enhanced capabilities necessary for the protection of our Nation’s critical infrastructure.

Participants will identify physical and cybersecurity concerns impacting overall infrastructure security posture, examine integrated physical and cybersecurity incidents and the evolving risks and impacts they pose to critical infrastructure, and explore resources that can be applied to improve security within an organization, business, or government entity. The target audience are critical infrastructure owners and operators and individuals responsible for physical and/or cybersecurity within their organization, including Federal, State, local, regional, tribal, and territorial government officials, and owners and operators of small businesses and non-profit organizations. This instructor-led course is 8 hours in length and offers 8 CEUs. For more information, contact nerrtc@teex.tamu.edu.

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.

Volunteer Opportunities

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? Looking for a way to earn CompTIA CEUs or (ISC)² CPEs? We’re always looking for members to teach one or more of the Security+ or CISSP domains. We provide the slides, but you can modify them as you see fit as long as your changes remain consistent with the official CompTIA or (ISC)² criteria. If you would like to volunteer to teach one of the Security+ or CISSP domains, or if you have questions, please contact our Training Committee leads at: Training@issa-cos.org.

If you have ideas/suggestions/requests for training initiatives, please email our Training Committee leads at: Training@issa-cos.org.
The AdGholas malvertising campaign infected thousands of computers per day

*Long-running malvertising operation tricked ad networks and malware scanners using steganography*

By Lucian Constantin, IDG News Service, July 28, 2016

Security researchers have shut down a large-scale malvertising operation that used sophisticated techniques to remain undetected for months and served exploits to millions of computers.

The operation, dubbed AdGholas, has been running since at least October 2015. According to security vendor Proofpoint, the gang behind it managed to distribute malicious advertisements through more than 100 ad exchanges, attracting between 1 million and 5 million page hits per day.

The Proofpoint researchers estimate that 10 to 20 percent of computers that loaded the rogue ads were redirected to servers hosting exploit kits -- web-based attack tools that attempt to silently exploit vulnerabilities in popular applications in order to install malware.

The malvertising code used a series of complex checks to ensure that the visiting computers are not virtual machines used by security researchers or by ad networks themselves to discover malware.

Other checks were used to filter victims based on their geolocation and to serve certain malware programs, typically online banking Trojans, only to users in specific regions. This was likely done on request by the cybercriminal gangs behind those Trojans that paid the AdGholas group to distribute their malware.

In order to make it even harder for ad networks and security scanners to discover the attacks, the AdGholas group used steganography -- the technique of hiding code inside images. The rogue ads contained images with encrypted JavaScript code inside that was only extracted and executed for selected computers passing the required checks.

This is the first time when the use of steganography has been observed in a malvertising attack, according to Proofpoint. The company's researchers worked with researchers from Trend Micro to deconstruct the attackers' technique and analyze it.

Read the rest here:
Closing the talent gap: How to build a skilled cybersecurity workforce


This article briefly describes some of the emerging DoD cybersecurity qualification policies and follow-on initiatives.

As technology continues to evolve and reel in consumers, threats to cybersecurity increase exponentially — continuing to fuel the game of good versus evil and increasing the need for more skilled professionals to secure and defend valuable information systems for the government and private sector.

Currently there are 209,000 cybersecurity positions across the U.S. that are unfilled. What makes workforce requirements for cybersecurity so difficult to match? What is deterring professionals from entering the field? And what specific skills are needed to combat these ever-changing virtual attacks in real time?

Local cybersecurity experts and businesses weighed in on the needs and solutions for the national workforce shortage.

STUMBLING BLOCKS

Nationwide, postings for cybersecurity positions have gone up 74 percent since 2011, according to a Peninsula Press analysis of numbers from the Bureau of Labor Statistics.

The nation needs more cybersecurity threat analysts, people who are experienced in understanding the who, why, where — and to some degree — the how of cyber, said Ed Rios, CEO of CyberSpace Operations Consulting.

“A sophisticated cybersecurity workforce must include training and experience for combating attacks beyond the IT firewall,” he said. “We have a shortage of security professionals who fully understand how to mitigate threats across the cyber spectrum, including understanding the root source of the threat combined with an in-depth comprehension of their own vulnerabilities and potential consequences.”

There’s also a lack of entry-level talent trained to get to work immediately, using available tools and tactics to defend systems, said Alex Kreilein, managing partner and CTO of SecureSet, a cybersecurity firm and training academy.

“Attackers change their tactics every day, so it makes sense for our national response to change as well,” he said. “The traditional method of long-form education is not yielding the types of results that offset attackers.”

LINKING EDUCATION AND INDUSTRY

For two weeks this month, STEM Education for Southern Colorado hosted a cybersecurity camp at Sand Creek High School, contracting with SecureSet to instruct educators and students in hands-on activities.

Nearly 30 students and 26 teachers from across the region attended Generation Cyber through a $100,000 grant from the National Security Association and the National Science Foundation. They participated in interactive challenges such as hacking a web camera to infiltrate an unsecured computer or network.

“I feel it’s important for students and educators to learn about cybersecurity because it’s not only an industry on fire, with stability and high-paying jobs, but a science that affects our everyday lives,” said Michelle Wallace, STEMsCO program manager. “From password protection, Internet of Things hacking and social engineering — cybersecurity is involved in our 21st century lives on a daily basis. It’s not just cybersecurity; it’s personal security.”

Matt Klausch, a senior at Widefield High School, competes on a CyberPatriot team at his school, a program developed by the Air Force Association to motivate youths to seek STEM careers.

He said he learned how easy it is to access and hack into household items, including by way of a smart refrigerator that allows buyers to connect their phone to the appliance to view the food inside.

“Because it’s easy for hackers to tap into your Wi-Fi,” he said, “I think it’s important for everyone to take a basic computer science class so they can protect their information and not randomly click on or download a link that is malicious.”

Owl Cybersecurity, a Denver-based startup founded in 2015, presented information to students and teachers. The company specializes in the Darknet and works with governments and private businesses to improve their security.

“As a company, we’re looking for qualified applicants — and not finding them,” said Katie Toren, director of marketing. “We’re trying to find ways to help get people excited about cybersecurity, explain to them what it is, what they can do with it and why it’s a fun career.”

Some students just aren’t aware that the industry exists, she said.

“Kids are not exposed to it in elementary, middle and high school,” Toren said, “This is why this camp is so great, because these are elementary, middle and high school teachers.”

Read the rest here:
Ransomware 2.0 is around the corner and it's a massive threat to the enterprise

By Teena Maddox, TechRepublic, July 26, 2016

Despite the efforts made to improve cybersecurity at many organizations, there are too many systems with aging infrastructure and vulnerabilities that leave companies at risk, with ransomware one of the most sinister threats, according to a new Cisco report.

Ransomware is a top concern because it's become an area of intense focus for cybercriminals due to its effectiveness at generating revenue. Once a cybercriminal hacks into a company's files and encrypts them, victims have little option but to pay the asking price for the code to decrypt their files. Ransomware is becoming more ominous as new versions are continually being developed.

"The landscape is simple. Attackers can move at will. They're shifting their tactics all the time. Defenders have a number of processes they have to go through," said Jason Brvenik, principal engineer with Cisco's security business group, discussing the Cisco 2016 Midyear Cybersecurity Report.

Cisco used data from its customers to create the report, since there are more than 16 billion web requests that go through the Cisco system daily, with nearly 20 billion threats blocked daily, and with more than 1.5 million unique malware samples daily, which works out to 17 new pieces of malware every second, Brvenik said.

Brvenik has the following recommendations for companies wanting to improve security:

- Improve network hygiene - Improve aging infrastructure to limit vulnerabilities.
- Integrate defenses - Use machine learning techniques combined with novel data views.
- Measure time to detection - Find out how long an attacker can live in your network before they are found.
- Protect your users everywhere they are - Protect users whether they're on a laptop, a smartphone, or another device. Don't just protect networks but protect users. They are the target.

The next step in the evolution of malware will be ransomware 2.0, which Brvenik said "will start replicating on its own and demand higher ransoms. You'll come in Monday morning and 30% of your machines and 50% of your servers will be encrypted. That's really a nightmare scenario."

Ransomware campaigns started out primarily through email and malicious advertising, but now some attackers are using network and server-side vulnerabilities as well. Self-propagating ransomware will be the next step to create ransomware 2.0, and companies need to take steps to prepare and protect their company's network, Brvenik said.

New modular strains of ransomware will be able to quickly switch tactics to maximize efficiency. For example, future ransomware attacks will evade detection by being able to limit CPU usage and refrain from command-and-control actions. These new ransomware strains will spread faster and self-replicate within organizations before coordinating ransom activities, according to the report.

The report detailed one widespread campaign that appeared to target the healthcare industry earlier this year. It used the Samas/Samsam/MSIL.B/C ("SamSam") ransomware variant, which was distributed through compromised servers. The attackers used the servers to move laterally through the network and compromise additional machines, which were then held for ransom, according to the report.

JexBoxx, an open source tool for testing and exploiting JBoss application services, had been used to allow the attackers to gain access to networks in the targeted companies. Once the attackers had access to the network, they encrypted multiple Windows systems using SamSam.

Overall, in all aspects of cybersecurity, there are too many companies with vulnerabilities that haven't been addressed. Out of 103,121 Cisco devices connected to the internet that were studied for the report, each device on average was running 28 known vulnerabilities. The devices were actively running known vulnerabilities for an average of 5.64 years, and more than 9 percent had known vulnerabilities older than 10 years, according to the report.

"In April, Cisco estimated that 10% of all JBoss servers worldwide were compromised. And they were compromised using readily available tools and old vulnerabilities. Adobe Flash is still a favorite. It gives a viable attack surface for them. And we see Microsoft Silverlight vulnerabilities. This means to us that people are opportunistizing those that work for them," Brvenik said.

Read the rest here:
Smartwatches not secure, give away PIN numbers

How you move your hand at an ATM when entering the PIN gives away the supposedly secure number to your sensor-packed wearable device, scientists say

By Staff, NetworkWorld, July 8, 2016

Sensors, such as accelerometers, found in wearable devices can be used to reverse engineer a human hand’s movements and trajectories while at an ATM, thus giving away the PIN code, researchers say.

The findings bring into question the fundamental security of smartwatches.

Malware installs on devices might be one way the newly discovered hack could work, the scientists say. The software would wait for a mark to use a secure system, such as a keypad-controlled enterprise server, for example, and then collect data from the gyroscope, magnometer, accelerometer and other sensors. (Devices use those sensors to measure fitness and so on.)

It would then send the harvested data back to the bandit who uses an algorithm to interpret the collected hand trajectories and map them into millimeter-accurate keypad numbers.

In testing, the crack was found to have “80 percent accuracy on the first try and more than 90 percent accuracy after three tries,” Binghamton University and the Stevens Institute of Technology say in a press release about the discovery.

The university tested 5,000 systems with 20 adults over 11 months.

A second way the same attack can be implemented is through a Bluetooth connection between the wearable device and the user’s smartphone. The criminal merely plucks the “fine-grained hand movement” raw data from the radio communication with a nearby sniffer and then runs the same mathematics.

Fitness fanatics often use a smartphone’s larger screen to view the watch-collected exercise data and see how well they’re doing—or not. Bluetooth is used for the connection.

“Distance and direction estimations between consecutive keystrokes” are provided through the hand movements in both scenarios. Then the team’s “Backward PIN-sequence Inference Algorithm” breaks the codes.

And it does it with “alarming accuracy without context clues about the keypad,” the university says. A lack of context is a big deal. The scientists say the malefactor doesn’t need to know details about the keyboard to perform the felonious deed.

"The threat is real, although the approach is sophisticated," says Yan Wang, paper co-author and assistant professor of computer science within the Thomas J. Watson School of Engineering and Applied Science at Binghamton.

However, the point is that "wearable devices can be exploited," Wang says in the release.

The problem is principally that security isn’t strong enough, the scientists say. Smartwatch “size and computing power doesn’t allow for robust security measures, which makes the data within more vulnerable to attack,” they say.

Indeed some argue that many internet-connected devices at the consumer level, like home IoT, overall aren’t secure. Experts say one reason is because the fast development cycle of the new genres doesn’t allow enough time for testing. And low profit margins in consumer products, such as home IoT devices, and conceivably wearable tech means corners may get cut.

In any case, encryption isn’t good enough in wearable devices where the “device and host operating system” meet, the Binghamton team says.

Read the rest here:
This Government Agency’s Cover-Up May Have Hindered US Cybersecurity

By Alton Martin & Riley Walters, The Daily Signal, July 25, 2016

The Chinese government may have hacked into computers at the Federal Deposit Insurance Corporation on multiple occasions between 2010 and 2013, according to a congressional report.

The report describes various instances of in which current or former FDIC employees inadvertently downloaded sensitive data to portable storage devices, which were later removed from the office. Rep. Lamar Smith, R-Texas, chairman of the U.S. House Science, Space, and Technology Committee, described the FDIC’s cybersecurity efforts as “lax” and asserted that “major improvements need to be made to the FDIC’s cybersecurity mechanism.”

The FDIC was originally established in 1933 to provide insurance for bank investments and create confidence in the American financial system.

The interim report was issued last Wednesday by the Republican majority of the U.S. House Science, Space, and Technology Committee.

However, the report’s most serious accusation addresses the agency’s handling of the hacks. According to the report, the FDIC not only failed to report major hacks, but also actively worked to “evade congressional oversight” during the congressional investigation.

The FDIC’s efforts to avoid congressional oversight included the agency’s top lawyer instructing employees not to discuss the hacks via email. The FDIC’s chief information officer at the time, Russ Pittman, also called on employees not to discuss the hack. The FDIC’s efforts were apparently an effort not to jeopardize current Chairman Martin Gruenberg’s impending congressional confirmation in 2012.

According to a source close to the investigation, the servers that were targeted indicate the hackers were seeking “economic intelligence.” These accusations follow the hacking of the Office of Personnel Management last year, which saw Chinese hackers obtain the personal records of 22 million current and former government employees.

In September 2015, the United States and China agreed not to engage in corporate cyber espionage and established a joint dialogue to discuss cybercrime. A report by FireEye cybersecurity firm indicated a decrease in Chinese cyber corporate espionage hacking since mid-2014. However, the report also claims Chinese cyberattacks were becoming much more targeted and aimed at specific infrastructure.

Read the rest here:
http://dailysignal.com/2016/07/25/this-government-agencys-cover-up-may-have-hindered-us-cybersecurity/
Today, the President approved a Presidential Policy Directive (PPD) on United States Cyber Incident Coordination. This new PPD marks a major milestone in codifying the policy that governs the Federal government’s response to significant cyber incidents.

Since the beginning of his Administration, President Obama has emphasized that malicious cyber activity poses a serious threat to the national and economic security of the United States. As set forth in the Cybersecurity National Action Plan, over the last seven and a half years the Administration’s cyber policy has been based on three strategic pillars: raising the level of cybersecurity in our public, private, and consumer sectors, in both the short and the long-term; taking steps to deter, disrupt, and interfere with malicious cyber activity aimed at the United States or its allies; and responding effectively to and recovering from cyber incidents.

Even as we have made progress on all three pillars, the United States has been faced with managing increasingly significant cyber incidents affecting both the private sector and Federal government. We have applied the lessons learned from these events, as well as our experience in other areas such as counterterrorism and disaster response. That experience has allowed us to hone our approach but also demonstrated that significant cyber incidents demand a more coordinated, integrated, and structured response. We have also heard from the private sector the need to provide clarity and guidance about the Federal government’s roles and responsibilities. The PPD builds on these lessons and institutionalizes our cyber incident coordination efforts in numerous respects, including:

- Establishing clear principles that will govern the Federal government’s activities in cyber incident response;
- Differentiating between significant cyber incidents and steady-state incidents and applying the PPD’s guidance primarily to significant incidents;
- Categorizing the government’s activities into specific lines of effort and designating a lead agency for each line of effort in the event of a significant cyber incident;
- Creating mechanisms to coordinate the Federal government’s response to significant cyber incidents, including a Cyber Unified Coordination Group similar in concept to what is used for incidents with physical effects, and enhanced coordination procedures within individual agencies;
- Applying these policies and procedures to incidents where a Federal department or agency is the victim; and,
- Ensuring that our cyber response activities are consistent and integrated with broader national preparedness and incident response policies, such as those implemented through Presidential Policy Directive 8-National Preparedness, so that our response to a cyber incident can seamlessly integrate with actions taken to address physical consequences caused by malicious cyber activity.

We also are releasing today a cyber incident severity schema that establishes a common framework within the Federal government for evaluating and assessing the severity of cyber incidents and will help identify significant cyber incidents to which the PPD’s coordination procedures would apply.

**Incident Response Principles**

The PPD outlines five principles that will guide the Federal government during any cyber incident response:

- **Shared Responsibility** – Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

- **Risk-Based Response** – The Federal government will determine its response actions and resource needs based on an assessment of the risks posed to an entity, national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

- **Respecting Affected Entities** – Federal government responders will safeguard details of the incident, as well as privacy and civil liberties, and sensitive private sector information.

- **Unity of Effort** – Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident.
• **Enabling Restoration and Recovery** – Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements with the need to return to normal operations as quickly as possible.

**Significant Cyber Incidents**

While the Federal government will adhere to the five principles in responding to any cyber incident, the PPD’s policies and procedures are aimed at a particular class of cyber incident: significant cyber incidents. A significant cyber incident is one that either singularly or as part of a group of related incidents is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

When a cyber incident occurs, determining its potential severity is critical to ensuring the incident receives the appropriate level of attention. No two incidents are the same and, particularly at the initial stages, important information, including the nature of the perpetrator, may be unknown.

Therefore, as part of the process of developing the incident response policy, the Administration also developed a common schema for describing the severity of cyber incidents, which can include credible reporting of a cyber threat, observed malicious cyber activity, or both. The schema establishes a common framework for evaluating and assessing cyber incidents to ensure that all Federal departments and agencies have a common view of the severity of a given incident, the consequent urgency of response efforts, and the need for escalation to senior levels.

The schema describes a cyber incident’s severity from a national perspective, defining six levels, zero through five, in ascending order of severity. Each level describes the incident’s potential to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. An incident that ranks at a level 3 or above on this schema is considered “significant” and will trigger application of the PPD’s coordination mechanisms.

**Lines of Effort and Lead Agencies**

To establish accountability and enhance clarity, the PPD organizes Federal response activities into three lines of effort and establishes a Federal lead agency for each:

• Threat response activities include the law enforcement and national security investigation of a cyber incident, including collecting evidence, linking related incidents, gathering intelligence, identifying opportunities for threat pursuit and disruption, and providing attribution. *The Department of Justice, acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF),* will be the Federal lead agency for threat response activities.


---

**Israeli researcher fans fears: here's another way to cross the airgap**

By Richard Chirgwin, The Register, June 24, 2016

Pity the weary sysadmin who's just finished silencing the loudspeakers in the company's computers to keep data behind the air gap: processor fans can also be used to whisper your secrets.

Israeli white-hat Mordechai Guri, who last year fiddled with firmware to transmit crypto keys from computers to feature phones on GSM frequencies, says fan speed can be modulated, creating an audio channel for data leakage.

As in his previous work, an attacker needs to be able to infect the target to plant the badware that gathers (for example) passwords from the keyboards and put that data into a modulated fan signal.

It's also a very slow channel: Guri's paper describing Fansmitter says the trick's been tested over distances of up to 8 metres, at a snail’s pace 900 bits per hour. Still: if all you want is someone's passwords, that's more than sufficient.

An ordinary smartphone has a good enough microphone to receive the data, he reckons.

Data can be modulated on either the amplitude (loudness) of the fan, or on its frequency, he writes, with the attacker choosing which is better based on the environment and how much is known about the target machine.

Read the rest here: http://www.theregister.co.uk/2016/06/24/israeli_researcher_fans_fears_heres_another_way_to_cross_the_airgap/
Chatbot lawyer overturns 160,000 parking tickets in London and New York

Free service DoNotPay helps appeal over $4m in parking fines in just 21 months, but is just the tip of the legal AI iceberg for its 19-year-old creator


An artificial-intelligence lawyer chatbot has successfully contested 160,000 parking tickets across London and New York for free, showing that chatbots can actually be useful.

Dubbed as “the world’s first robot lawyer” by its 19-year-old creator, London-born second-year Stanford University student Joshua Browder, DoNotPay helps users contest parking tickets in an easy to use chat-like interface.

The program first works out whether an appeal is possible through a series of simple questions, such as were there clearly visible parking signs, and then guides users through the appeals process.

The results speak for themselves. In the 21 months since the free service was launched in London and now New York, Browder says DoNotPay has taken on 250,000 cases and won 160,000, giving it a success rate of 64% appealing over $4m of parking tickets.

“I think the people getting parking tickets are the most vulnerable in society. These people aren’t looking to break the law. I think they’re being exploited as a revenue source by the local government,” Browder told Venture Beat.

The bot was created by the self-taught coder after receiving 30 parking tickets at the age of 18 in and around London. The process for appealing the fines is relatively formulaic and perfectly suits AI, which is able to quickly drill down and give the appropriate advice without charging lawyers fees.

Browder intends to expand DoNotPay to Seattle next. But having started with parking tickets, Browder’s next challenge for the AI lawyer is helping people with flight delay compensation, as well as helping the HIV positive understand their rights and acting as a guide for refugees navigating foreign legal systems.

At the same time, Browder is exploring a developer platform that only requires legal knowledge, not a coding background, which could spawn further useful chatbots to help dispense simple legal advice without exorbitant fees.

Read the rest here:

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
ISSA photos are courtesy of our Chapter Photographer Warren Pearce.
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: doncreamer-issa@q.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Kerberos?

If you ever think that mythology is boring, or serious business, or whatever, just remember that Cerberus, the hell-hound and guard dog of the underworld, comes from the Proto-Indo-European work Kerberos, which became the Greek word Κέρβερος, which got changed into Cerberus when it went from Greek to Latin.

“Kerberos” means “spotted.”

That’s right.

Hades, Lord of the dead, literally named his pet dog “Spot”.

And that concludes today’s lesson.