Also, please note that our lunch meeting this month will be held at the Hewlett-Packard Enterprise (HPE) facility located at 305 South Rockrimmon Blvd. The dinner meeting will be at the Disabled American Veterans facility at 6880 Palmer Park Blvd. Additional info will be on our website and in emails soon.

Our May Mini-Seminar will be on Saturday, May 19th, at College America. Additional info will be posted to our website and in emails soon.

Planning is already in progress for these events, and we could use your help. If you are interested in helping with these events, or any other event, please let me know (president@issa-cos.org).

We still have a few vacant Board Officer Positions: Deputy Recorder, Deputy Treasurer, Deputy Communications, and Director of Professional Outreach. Job descriptions for these positions can be found on our website, under "NEWS", in the "Members (Restricted)" area. You’ll need to log into our website to access this area. If you’re interested in any of these positions, or would like additional information, please contact me.

(Continued on page 4)
Cops take dead man’s smartphone to his corpse in attempt to unlock it

By Cyrus Farivar, Ars Technica, April 29, 2018

In a very unusual move, police detectives in Largo, Florida, recently went to a local funeral home and located the body of a man named Linus Phillip. The 30-year-old had died days earlier at the hands of a different Largo officer. The detectives then attempted to use the fingers on Phillip’s body to unlock his own smartphone, which had been recovered from the scene. Their efforts were not successful.

For years, law enforcement officials nationwide have said that they struggle with the so-called “Going Dark” problem—the idea that strong encryption on smartphones is making it significantly more difficult for police to access data held there.

As the two officers approached the Nissan, they believed that they smelled marijuana from the car as Phillip got out and left the driver’s side door open.

After a brief conversation, police say, Phillip jumped back into the driver’s seat of his own car and tried to drive away.

One of the officers, Matthew Steiner, was “trapped halfway” in the Nissan as Phillip tried to quickly drive backwards and forwards (presumably as a way to shake Steiner loose), all while the driver’s side door remained open. (The other officer, Prentice Ables, had already gotten out of the way.)

As he was being “dragged” by the car, Steiner shot at Phillip four times in self-defense. Steiner then was finally freed from the car, but was “brushed” by the moving car door.

Moments later the Nissan, with Phillip at the wheel, hit a thick post before stopping between a pair of gas pumps. With Phillip subdued, the officers began offering medical treatment and summoned paramedics. He was later pronounced dead at Largo Medical Center.

According to the paper, police eventually found a “significant amount” of cocaine and marijuana in Phillip’s car.

“At the time, the officer felt he was in peril for his own life and took action,” Lt. Randall Chaney told reporters at a news conference held Friday night, hours after the incident. “It stopped the action of the suspect at the time, and it may very well have saved people’s lives in the parking lot that night.”

Probably legal

Days later, two police detectives arrived at the Sylvan Abbey Funeral Home in Clearwater. Phillip’s fiancée, Victoria Armstrong, happened to be there at the time.

Somehow, the officers were allowed access to Phillip’s body, where they “tried to unlock the phone by holding the body’s hands up to the phone’s fingerprint sensor.”

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.

It’s been a quiet month on the membership front. Our membership continues steady around the 500 mark as of the end of April. We have lots of upcoming activities scheduled between meetings, training and mini-seminars. Please watch the Newsletter, communications and eVites to ensure you stay aware of what’s going on in the chapter. Also, please continue to refer new members to the chapter. Referrals are a critical part of developing new members for ISSA. As always, if you have any membership questions don’t hesitate to contact me.

Thanks,

David Reed

Membership Committee Chairman
dreed54321@comcast.net

<table>
<thead>
<tr>
<th>New Members</th>
<th>April</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wesley Smith</td>
<td></td>
</tr>
<tr>
<td>Stacie Squires-Neale</td>
<td></td>
</tr>
<tr>
<td>Charles Harms</td>
<td></td>
</tr>
<tr>
<td>Robert Boston III</td>
<td></td>
</tr>
<tr>
<td>Mariyam Zaheer</td>
<td></td>
</tr>
<tr>
<td>Dustin Ruland</td>
<td></td>
</tr>
</tbody>
</table>

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
The Chapter mini-seminar on April 28 had two great speakers. Patrick Lynch spoke eloquently on the importance of cybersecurity and of risk management. Stuart Gentry introduced the attendees to some basics of reverse engineering software.

Our next meeting will be on Saturday, May 19. Stuart will take some time to help us set up our own cybersecurity laptops with critical tools. This will be the basis for lots of future lectures on using tools like Wireshark, Nmap, and Kali Linux.

The second part of the session will introduce Quantum Computing. Mark McGough has been studying this for years. This presentation will also be part of a series. Depending on how well we understand computing (Mark McG says he can take it to the 3rd grade level, so there is hope for us), Mark will take us into the world of quantum cryptography at a future mini-seminar.

April's Security+ Exam Review Seminar, which covered the CompTIA SY0-401 exam criteria, was very successful. A special thanks to the volunteer instructors: James Asimah, Frank Gearhart, Ralph Hoefelmeyer, and Chuck Wright. The seminar cannot happen without them. If you are an ISSA member and, at a minimum, Security+ certified, you too can be an instructor. This is a terrific opportunity for those just starting out with instructing, as well as, for those who have experience. You also get CEUs/CPEs. If interested in instructing at the June Security+ seminar or future seminars, please contact the Training Team at trainingcommittee@NETORG3807428.onmicrosoft.com.

The next Security+ Exam Review Seminar will be held June 2 & 9. This will be the first seminar to cover the updated CompTIA exam criteria, SY0-501. The Training Committee is so very grateful to the volunteers who are updating the Security+ domain slide sets to the SY0-501 criteria. This is a big effort as the updates take time and research. These updates not only benefit our ISSA-COS chapter, but provides a great value to so many cyber security professionals with assistance in passing the Security+ exam and obtaining this all important certification. Our sincere appreciation goes to the volunteers who are doing the domain updates: Lisa Gilbert, Ralph Hoefelmeyer, Anna Johnston, Tom Oliphant, Chuck Wright, and Dave Zarsky.

Mark Heinrich & Susan Ross

Colleen

A Note From Our President

(Continued from page 1)

information, please let me know (president@issa-cos.org).

We also could use some help organizing our Mini-Seminars. Mini-Seminars are held on a Saturday morning, from 9am to noon, about seven to eight times each year. We’d like to have one more person join our team of organizers to help organize one or two Mini-Seminars. You’ll receive three CEUs/CPEs for every mini-seminar you organize and attend. If you’re interested in joining our team of organizers for training events, please let me or our Training leads (training@issa-cos.org) know.

Colleen

Training Team Update

The Chapter mini-seminar on April 28 had two great speakers. Patrick Lynch spoke eloquently on the importance of cybersecurity and of risk management. Stuart Gentry introduced the attendees to some basics of reverse engineering software.

Our next meeting will be on Saturday, May 19. Stuart will take some time to help us set up our own cybersecurity laptops with critical tools. This will be the basis for lots of future lectures on using tools like Wireshark, Nmap, and Kali Linux.

The second part of the session will introduce Quantum Computing. Mark McGough has been studying this for years. This presentation will also be part of a series. Depending on how well we understand computing (Mark McG says he can take it to the 3rd grade level, so there is hope for us), Mark will take us into the world of quantum cryptography at a future mini-seminar.

April’s Security+ Exam Review Seminar, which covered the CompTIA SY0-401 exam criteria, was very successful. A special thanks to the volunteer instructors: James Asimah, Frank Gearhart, Ralph Hoefelmeyer, and Chuck Wright. The seminar cannot happen without them. If you are an ISSA member and, at a minimum, Security+ certified, you too can be an instructor. This is a terrific opportunity for those just starting out with instructing, as well as, for those who have experience. You also get CEUs/CPEs. If interested in instructing at the June Security+ seminar or future seminars, please contact the Training Team at trainingcommittee@NETORG3807428.onmicrosoft.com.

The next Security+ Exam Review Seminar will be held June 2 & 9. This will be the first seminar to cover the updated CompTIA exam criteria, SY0-501. The Training Committee is so very grateful to the volunteers who are updating the Security+ domain slide sets to the SY0-501 criteria. This is a big effort as the updates take time and research. These updates not only benefit our ISSA-COS chapter, but provides a great value to so many cyber security professionals with assistance in passing the Security+ exam and obtaining this all important certification. Our sincere appreciation goes to the volunteers who are doing the domain updates: Lisa Gilbert, Ralph Hoefelmeyer, Anna Johnston, Tom Oliphant, Chuck Wright, and Dave Zarsky.

Mark Heinrich & Susan Ross
Next Mentorship Group Meeting will be in July. Thanks to all who attended last month's meeting. For more information about the program, please email Melissa Absher at mentorship@issa-cos.org.

Mission Statement

Provide interested mentees at any stage of their information security career lifecycle with access to mentors who share their knowledge and experience in ensuring the confidentiality, integrity, and availability of information resources throughout a variety of industries.

Overview

The ISSA-COS Mentorship Program is designed to be mentee driven. Mentees determine the number of mentors they meet with depending on their questions, needs, and availability. The goal is to provide mentees with quality mentoring opportunities in a professional and problem solving environment. There will be group meetings quarterly for all mentors and mentees to meet, greet, and discuss information security. Individual meetings between mentees and mentors will be scheduled throughout the year determined by the mentee and mentor. Mentees and mentors are expected to prepare for individual meetings by writing down questions and discussion topics prior to the meeting. e-Mentoring is also an option for those who need remote options. Small group meetings to discuss specific topics and field trips to companies and organizations will be scheduled ad hoc.
ISSA Fellow Program

2018 Fellows Cycle Closing Soon

The Colorado Springs ISSA Chapter has over 500 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Erik Huffman at erik.huffman@independence.edu to coordinate the process. Erik is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. Applications will be accepted until June 17, 2018 at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2018 ISSA International Conference.

Familiarize yourself with the Fellow Program, and the submission guidelines. If you have questions, contact Erik or The ISSA Fellow Manager or call 866-349-5818 (US toll free) extension 4082.

To Become a Senior Member

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

Senior Member Qualifications

• 5 years of ISSA membership

• 10 years relevant professional experience

All Senior Member applications require an endorsement from their home chapter to qualify.

Click here to access the Senior Member application.

Click here for the Senior Member endorsement form.

To Become a Fellow or Distinguished Fellow

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow. Please contact Erik and become familiar with the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

Fellow Qualifications

• 8 years of association membership.

• 3 years of volunteer leadership in the association.

• 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty developing and teaching courses.

(Continued on page 7)
All Fellow applications require a nomination to qualify.

Click here to access the Fellow application.
Click here to nominate a Fellow.
Click here to submit a Fellow letter of recommendation.

Distinguished Fellow Qualifications

- 12 years association membership.
- 5 years of sustained volunteer leadership in the association.
- 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability.

All Distinguished Fellow applications require a nomination to qualify.

Click here to access the Distinguished Fellow application.
Click here to nominate a Distinguished Fellow.
Click here to submit a Distinguished Fellow letter of recommendation.

Please help us identify candidates that we can recognize in our chapter! Please contact:

Erik Huffman
Awards & Recognition Committee Chair
erik.huffman@independence.edu

Atlanta pays $2.6 million for cybersecurity issues stemming from $51,000 ransomware attack

By Jason Axelrod, American City & County, April 30, 2018

Following a ransomware attack in March, Atlanta has spent over $2 million to ensure that the city will be well protected against cyberattacks in the future.

On March 22, the SamSam ransomware attack struck Atlanta, causing outages across city servers, American City & County reports. The perpetrators demanded $51,000 in Bitcoin as ransom to stop the attack.

City employees have struggled to recover from the attack in the weeks since. One council member lost 16 years worth of digital data, and some city employees were still using paper forms 10 days after the attack first struck, according to The Hill.

To some officials, the susceptibility may not have come as a surprise. City auditor records show that Atlanta had failed a security compliance assessment in January, Wired reports.

“Dedicating resources to formalize and document information security management processes would prepare the city for certification, and, more importantly, provide assurance that the city is adequately managing and protecting its information assets,” the audit report states, per Wired.

While Atlanta officials never paid the SamSam ransom, the city has hefty bills to pay from the attack’s fallout and recovery from it, according to ZDNet.

Between March 22 and April 2, the city procured eight emergency contracts that valued $2,667,328, Wired reports. The city spent an additional $50,000 on crisis communication services from communications marketing firm Edelman and $600,000 on incident response consulting from professional services firm Ernst & Young.

Read the rest here:
U.S. DoD Hopes To Stamp Out Threats With Bug Bounty Program

By Lindsey O'Donnell, ThreatPost, April 2, 2018

The U.S. Department of Defense is doubling down on routing out vulnerabilities in its massive government systems. On Monday, the DoD announced it was expanding its bug bounty program to include the agency’s massive Defense Travel System.

The “Hack the DTS” program launched in partnership with bug bounty firm HackerOne. It targets potential threats found in a Department of Defense enterprise system called Defense Travel System (DTS). The DTS serves the DoD’s massive travel services’ bureaucracy and is responsible for everything from generating itineraries to reimbursements for millions of global DoD travelers.

“The DoD has seen tremendous success to date working with hackers to secure our vital systems, and we’re looking forward to taking a page from their playbook,” said Jack Messer, project lead at Defense Manpower Data Center in a statement. “We’re excited to be working with the global ethical hacker community, and the diverse perspectives they bring to the table, to continue to secure our critical systems.”

“The scale of users, volume of travel booked, and sensitive information it is responsible for maintaining makes DTS both a compelling asset for researchers and a priority for DoD to harden its security,” Reina Staley, chief of staff and co-founder of Defense Digital Service, told Threatpost.

Up to 600 eligible white-hat hackers will be invited to participate in the challenge, according to HackerOne. To be eligible to participate in this latest bug bounty challenge by the DoD, hackers must be U.S. taxpayers or a citizen eligible to work in the United Kingdom, Canada, Australia, or New Zealand. U.S. government active military members and contractor personnel are also eligible to participate but are not eligible for financial rewards, said the DoD.

The bug bounty program opened registration on April 1, and will continue until April 29. HackerOne would not disclose the financial rewards tied to the program, but said that in May the company will announce the total money paid.

The program is part of a push by the U.S. Department of the Defense to explore new approaches to its security, and to adopt the best practices used by the most successful and secure software companies in the world. “The intent of our Hack the Pentagon program is to enable the entire Department of Defense to run both public and private bug bounties against websites, applications, and internal systems that are critical to DoD operations,” said Staley.

“Hack the DTS” is the latest effort by the government to step up its cybersecurity measures. In 2016, the “Hack the Pentagon” program was first launched – and since then over 3,000 vulnerabilities have been resolved in government systems. That includes invite-only programs like “Hack the Air Force” in 2017 which resulted in 207 reports and $130,000 in rewards for hackers, and “Hack the Army” in 2016 which resulted in 138 resolved vulnerabilities and $100,000 in rewards for hackers.

Read the rest here:

NIST Releases Version 1.1 of its Popular Cybersecurity Framework

By Staff, NIST, April 16, 2018

The U.S. Commerce Department’s National Institute of Standards and Technology (NIST) has released version 1.1 of its popular Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework.

“Cybersecurity is critical for national and economic security,” said Secretary of Commerce Wilbur Ross. “The voluntary NIST Cybersecurity Framework should be every company’s first line of defense. Adopting version 1.1 is a must do for all CEO’s.”

The framework was developed with a focus on industries vital to national and economic security, including energy, banking, communications and the defense industrial base. It has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state and local governments.

Read the rest here:
Your Nosy Amazon Alexa Can Now Interrogate You
By Paula Bolyard, PJ Media, April 49, 2018

Rohit Prasad, vice president and head scientist for Amazon Alexa, said this week in an interview posted at Amazon's blog that AI holds promise and will have "deep societal impact and will help humans learn new skills that we can't even imagine today." He also announced that socialbots—currently being tested by Amazon Alexa users—are capable of holding a 10-minute "coherent" conversation.

In the next five years, he said, "we will see conversational AI get smarter on multiple dimensions as we make further advances with machine learning and reasoning." In addition, "we will see Alexa become more contextually aware in how she recognizes, understands, and responds to requests from users. Alexa will become smarter more quickly as unsupervised learning will dominate how she learns."

Amazon is well on its way to the goal of creating a socialbot that can hold a 20-minute conversation. The company recently held a competition for university students "to advance human-computer interaction." The teams, which competed for $3.5 million in prizes, were tasked with creating socialbots that were able to converse "coherently and engagingly with humans on a range of current events and popular topics such as entertainment, sports, politics, technology, and fashion." Participating teams each received a $250,000 research grant, Alexa-enabled devices, and free Amazon Web Services (AWS) to aid in project development.

Amazon announced the winners in November of last year. The first place team, from the University of Washington, created a socialbot that was able to converse for 10 minutes and 22 seconds. The team was awarded $500,000 to share among team members.

The second place team, from Czech Technical University in Prague, was awarded $100,000. The team that came in third, from Heriot-Watt University in Edinburgh, Scotland, will share a prize of $50,000.

Amazon gave an example of a socialbot conversation:

User: Let's chat about the Mars Mission.
Socialbot: There are multiple Mars missions, some public and some private.
User: Who do you think will succeed?
Socialbot: I think more than one will succeed. The first one to get to Mars will open the doors for others.

On my second try, my conversation with the first place socialbot from the University of Washington went like this:

Alexa: How are things?
Me: Fine.
Alexa: That's great how about we get to know each other now?
Me: OK.
Alexa: Which character from the lion king would suit you better: Timon or Pumba?
Me: Timon
Alexa: Interesting. For me, Timon suits me better. Do you have a vivid imagination?
Me: Yes.
Alexa: That's cool. I'm not sure if I have a vivid imagination. Do you usually like "Hoarders"?
Me: No.
Alexa: Personally, I prefer "Law and Order." If you could time travel, would you go to the past or to the future?
Me: The past.
Alexa: I think I'd go back to the future if I could. Do you feel like you do not have a good imagination?
Me: No.
Alexa: I think I imagine that I don't have a good imagination. At Thanksgiving do you eat pecan pie or pumpkin pie?

The bots still have a long way to go, but they are surprisingly more advanced than I expected, and, quite honestly, a little creepy.

On my second try, my conversation with the first place socialbot from the University of Washington went like this:

Alexa: How are things?
Me: Fine.
Alexa: That's great how about we get to know each other now?
Me: OK.
Alexa: Which character from the lion king would suit you better: Timon or Pumba?
Me: Timon
Alexa: Interesting. For me, Timon suits me better. Do you have a vivid imagination?
Me: Yes.
Alexa: That's cool. I'm not sure if I have a vivid imagination. Do you usually like "Hoarders"?
Me: No.
Alexa: Personally, I prefer "Law and Order." If you could time travel, would you go to the past or to the future?
Me: The past.
Alexa: I think I'd go back to the future if I could. Do you feel like you do not have a good imagination?
Me: No.
Alexa: I think I imagine that I don't have a good imagination. At Thanksgiving do you eat pecan pie or pumpkin pie?

Read the rest here: https://pjmedia.com/trending/amazon-alexa-can-now-conduct-lengthy-conversation-using-ai-socialbot/
The Do’s and Don’ts of Industrial IoT

Your boss wants to start an IoT project—what next?

By Stacey Higgenbotham, IEEE Spectrum, April 25, 2018

In a home or on a manufacturing floor, there’s no point in connecting something just so it’s online. You must have a reason.

Andy Rhodes, the former vice president and general manager for Dell’s Internet of Things (IoT) commercial sales division, once told me that he no longer takes phone calls from companies asking for “some IoT.” If the company doesn’t know what it wants to do with connected devices, it isn’t ready for a sales talk.

So how does a management team decide what it wants from the IoT?

There are two paths here. The first is to start small with a project that can offer a short-term return on investment (ROI). In a factory, this could mean installing cameras and sensors on a manufacturing line to replace human spot-checkers. Cities might install sensor-infused LED lighting to reduce energy costs.

The second path is a bit more visionary: Build a platform or product that can change your entire business model. For example, in 2015 Emerson Climate Technologies launched a new connected product in its HVAC business. With US $100 worth of sensors per home, the HVAC installer and Emerson could guarantee a period of time that a customer’s heating or cooling system would operate before needing repairs.

The ROI on this project is still unclear. But the idea was that tracking how hard the AC unit was running, and how long it takes to cool a home, could change Emerson’s business model from offering a product (HVAC units) to delivering a service.

However, Emerson’s client would have to add sensors, connectivity, and a gateway. And that requires labor at every point, which means it doesn’t scale in the way that traditional IT projects scale.

Upal Basu, general partner at NGP Capital, is concerned that focusing on short-term ROI leaves a lot of money on the table. He says the value in IoT deployments comes from data gathered by sensors—not from some centralized platform.

But a long-term approach is far more costly to execute. Which is why most companies will try to tweak small production lines or other minor functions within their businesses first.

Once a company has decided on a problem to solve—whether it’s saving energy by turning off lights or using sensors to gather information on a factory floor—the next step is to figure out who has done a similar project and talk to them about their process.

Peter Zornio, chief technology officer at Emerson Automation Solutions, says most clients turn to his team to understand how Emerson’s automated plant operations would work for other facilities.

“Unless you have a sparky operations guy who is reading about this—they may come to you with a specific example and solution—most customers come to us because we’ve already done this,” he says.

Read the rest here:

How to Steal Someone's Identity in 45 Minutes

By Paul Wagenseil, Tom’s Guide, April 19, 2018

You can totally steal someone’s identity after only 45 minutes of online research, a security expert said Wednesday (April 18) at the RSA Conference here.

Zee Abdelnabi, a cyber-risk manager with one of the Big Four accounting firms, demonstrated how she selected a target at random -- a middle-aged Midwestern man -- and decided to find out everything she could about him.

Within 45 minutes, Abdelnabi had learned where the man worked, his age, his date of birth, his wife's name, his previous wife's name, where he went to high school, where he lived and the names and ages of his children.

"Social media is an amazing tool for harvesting information,” she said.

Read the rest here:
Risk Management Framework (RMF) – Frequently Asked Questions (FAQ) 
(DSS Edition)

1. **When should Industry submit for reauthorizations?** Industry reauthorization submissions should be submitted 60 - 90 days before the current Authorization to Operate (ATO) expires. DSS personnel must: 1) Review the System Security Plan (SSP); 2) Conduct an assessment; 3) Allow for interaction with Industry for potential corrections/updates to submitted SSPs. Note: The DSS goal is to make authorization decisions within 30 days.

2. **Can Industry continue to operate systems after an ATO expires?** No. Once an ATO expires, Industry must cease processing on that system. If Industry submitted a complete reauthorization package 60-90 days prior to ATO expiration and DSS was unable to process the package due to workload, then DSS will determine if a short term (Limited) ATO may be issued. Communication between the Information System Security Manager (ISSM) and the local DSS Information Systems Security Professional (ISSP) is the key to successfully achieving an ATO reauthorization. Waiting until the day before an ATO expires to engage will ensure the process fails. A short term ATO is not automatic and will involve input from the local Regional Authorizing Official (AO) representatives. It is incumbent on Industry to submit a timely and complete reauthorization package.

3. **Is the ODAA Process Manual still effective?** No. As of January 1, 2018, the Defense Security Service Assessment and Authorization Process Manual (DAAPM) Version 1.2 will be used for all classified systems seeking authorization and/or re-authorization.

4. **Are Data Transfer Agents (DTA) considered privileged users?** Yes. Privileged users include anyone who conducts data transfers, including low to high.

5. **Is Industry required to review classification guidance when completing Risk Assessment Reports (RAR) and Plan of Action and Milestones (POA&M)?** Yes. Vulnerabilities identified in the Risk Assessment Report and/or the POA&M are subject to the Security Classification Guide (SCG) for that program. SCGs are required for every program per NISPOM 4-103 and 7-102.

6. **Will DSS publish a new list of Security Relevant Objects (SROs)?** No. DSS will no longer publish a list of Security Relevant Objects (SROs) to be audited. The ISSM must work with the Information Owner (IO)/Information System Owner (ISO) to determine what files are most appropriate to audit in order to mitigate the specific threats and vulnerabilities unique to the system.

7. **Can audit correlation controls be manual?** Yes. Audit correlation controls can be manual; they are meant to be a discussion between different security entities to determine if there is a pattern of security violations and insider threat concerns. Examples: 1) A pattern of similar software failures can point to a need to roll back a security patch; 2) Security violations from one individual in different areas might be correlated with Human Resource (HR) records.

Why Hackers Love Healthcare

By Allan Alford, Dark Reading, April 26, 2018

Much like the rest of the world, healthcare organizations are shifting work to cloud services in order to improve accessibility and patient care. However, the migration of these workloads and moving valuable information such as PHI (personal health information) and PII (personally identifiable information) to the cloud has also led to cybercriminals taking a particular interest in the industry.

The number of ransomware and other malware attacks is rising incredibly fast in the healthcare industry, putting human lives as well as critical data at risk. From 2011 through 2014, the sector — including hospitals, labs, pharmacies, drug companies and outpatient clinics — experienced the highest number of data breaches of all industries. What makes these organizations such a popular target?

1. **Highly Valuable Data**

One of the key aspects making healthcare organizations a top target is the value of their data. Commonly, a single stolen credit card number yields an average $2,000 profit and quickly becomes worthless. Healthcare data, however, such as PHI or PII, is extremely valuable on the black market.

A single PHI file, for example, can yield a profit of up to $20,000. This is mainly because it can take weeks or months for a healthcare data breach to be discovered, enabling cybercriminals to extract much more valuable data. Moreover, because healthcare data can contain dates of birth and Social Security numbers, it is much more difficult or even impossible to change, so thieves can take advantage of it for a longer period of time.

2. **Lack of IT Investment and Training**

Another reason the healthcare industry is popular among cybercriminals is its systematic underinvestment in IT security. Most healthcare organizations spend just 3% of their IT budgets on security, while the SANS Institute — the largest provider of cybersecurity training and certifications — recommends spending at least 10%.

For most healthcare organizations, security is often an afterthought. They don’t provide regular cybersecurity training for their employees, which could help reduce insider threats. For example, 18% of healthcare employees say they’re willing to sell their login credentials for between $500 and $1,000. And about one-quarter of healthcare employees know someone in their organization who has engaged in this practice.

To address employee-related cyber vulnerabilities, it’s important to note that while training is essential, it won’t magically protect patients’ digital data. Although some hospitals struggle to deploy the most basic IT security measures, such as intrusion detection and the ability to wipe lost or stolen devices, it is imperative that basic cyber hygiene practices are coupled with ongoing training to both protect well-intended employees and mitigate future data loss from those seeking to profit.

3. **Highly Connected Systems**

Having shifted workloads to the cloud, healthcare organizations have highly connected systems that run the risk of being deeply affected even if the attack takes place on smaller, partial systems. In other words, a cyberattack in one place could bring down the entire system. In May 2017, the WannaCry ransomware attack forced multiple hospitals across the United Kingdom to turn away ambulances transporting patients and cancel surgeries that were within minutes of starting. Even basic processes like admitting patients and printing wrist bands were compromised.

The impact of WannaCry illustrates how important it is for healthcare organizations to be able to function and provide patient care during a cyberattack. After all, lives are at risk, meaning there’s a general urgency to get back to business as soon as possible. For attackers, this urgency makes it extra tempting to target healthcare organizations, because they assume it will make them more likely to pay the ransom to reverse the infection.

**Fighting Back**

What can the healthcare industry do to mitigate cyber threats? To begin with, the industry must realize that cybersecurity is human-centric. Gaining insight into the normal rhythm of users’ behavior, for example, or the flow of data in and out of the organization improves risk response. Additionally, the industry should be aware that cybersecurity isn’t just the responsibility of the IT department: everyone should be aware of the risks, from management down to brand-new contract staff.

Healthcare security professionals need to understand the threats they face and the regulations they must comply with, and they must be provided with best practices for strengthening cybersecurity defenses. This means implementing comprehensive security awareness training that educates all personnel on current threats, red flags to look for in an email message or web link, how to avoid infection, and what to do in case of an active exploit. And since the threat landscape is constantly changing, training should be repeated and updated on a regular basis.

Read the rest here: https://www.darkreading.com/endpoint/why-hackers-love-healthcare/a/d-id/1331537
FDA Reveals New Plans for Medical Device Security

By Eduard Kovacs, Security Week, April 20, 2018

The U.S. Food and Drug Administration (FDA) this week announced its medical device safety action plan, which includes seeking additional funding and authorities that would help it improve cybersecurity in the healthcare industry.

The FDA’s plan focuses on five key areas and medical device cybersecurity is one of them. As part of its efforts to keep up with emerging threats and vulnerabilities, the agency wants the authority to require medical device manufacturers to include updating and patching capabilities into the design of their products.

The organization also wants vendors to create a “Software Bill of Materials,” which should help medical device customers and users determine which systems may be impacted by vulnerabilities.

“The additional authorities we seek are to further strengthen medical device security by directly addressing challenges healthcare delivery organizations and providers have encountered as a result of cyber campaigns and attacks such as WannaCry,” an FDA spokesperson told SecurityWeek.

The agency would require that “new devices entering the market have a demonstrated capability of patchability and updatability built into the design architecture of the device, and that a patch management process and plan is provided by the manufacturer for premarket review,” the spokesperson said.

As for the Software Bill of Materials, the measure is inspired by one of the recommendations made recently by the Health Care Industry Cybersecurity Task Force. A bill of materials would be issued for each piece of medical technology to describe its components and the risks associated with those components, which can help users understand the impact of certain threats and vulnerabilities.

The FDA also plans on updating its premarket guidance for medical device cybersecurity to better protect against moderate risks, which it has described as ransomware and other attacks that could disrupt clinical operations and delay patient care, and major risks, such as the remote exploitation of a vulnerability that can be used in a “multi-patient, catastrophic attack.”

The agency’s plans also include requiring companies to adopt policies and procedures for coordinated disclosure of vulnerabilities.

Read the rest here: https://www.securityweek.com/fda-reveals-new-plans-medical-device-security

ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

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

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.
By Kevin Townsend, SecurityWeek, April 19, 2018

Thirty-four major tech and security companies have aligned themselves and signed the Cybersecurity Tech Accord, what they claim is a "watershed agreement among the largest-ever group of companies agreeing to defend all customers everywhere from malicious attacks by cybercriminal enterprises and nation-states."

"The devastating attacks from the past year demonstrate that cybersecurity is not just about what any single company can do but also about what we can all do together," said Microsoft President Brad Smith. "This tech sector Accord will help us take a principled path towards more effective steps to work together and defend customers around the world."

The Accord makes commitments in four specific areas.

First, the companies say they will mount a stronger defense against cyberattacks, and will protect all customers globally regardless of the motivation of the attack.

Second, the companies claim they will not help governments launch cyberattacks against innocent citizens, and will protect their products against tampering or exploitation at every stage of development, design and distribution.

Third, the companies promise to do more to empower users to make effective use of their products with new security practices and new features.

Fourth, verbatim, "The companies will build on existing relationships and together establish new formal and informal partnerships with industry, civil society and security researchers to improve technical collaboration, coordinate vulnerability disclosures, share threats and minimize the potential for malicious code to be introduced into cyberspace."

A problem with the Accord, that many have already noted, is that it comprises fine words with no defined deliverables and possibly impossible intentions. It has no teeth. The first commitment is something that users could be excused for thinking they have already paid for in buying or licensing the signatories' products. The third, again, should be part and parcel of selling security products -- although it has received some support.

"Separate from the fact that some of the major social networks and cloud operators are missing [think, for example, Google and Amazon]," David Ginsburg, VP of marketing at Cavirin, told SecurityWeek, "the key to any meaningful outcome is better communication to users of how to use the security capabilities within the various vendors' tools. In several cases, the capabilities are there, but they are too difficult to deploy; or, in some cases, tools from multiple vendors will provide contradictory guidance. This practical aspect is tremendously important."

The second commitment is a little more complex. No company can disregard the law in its own country. Individual governments have the right and ability to pass whatever laws they wish, subject only to any overriding constitutional limitations. So, for example, once Brexit is finalized, the UK government would be able to insist on backdoors in the UK without fear of denial from the EU constitution.

Challenged on whether this commitment meant that the signatories would go against the U.S. government, or the British government or the Australian government or whoever, Microsoft president and chief legal officer, Brad Smith took the argument away from the Five Eyes nations.

"If you look at the world today," Smith said, "the biggest attacks against private citizens are clearly coming from a set of governments that we know well. It was North Korea, and a group associated with it, that launched the WannaCry attack last year... We saw the NotPetya attack launched against the country of Ukraine. Those are the big problems that we need to solve."

But it is doubtful that a group of tech companies could influence the governments of North Korea (WannaCry) and Russia (NotPetya); while it is equally doubtful that collaboration between the signatories could have detected and stopped the spread of WannaCry.

It is concerns such as this that are behind a degree of cynicism. One security executive -- preferring to remain anonymous -- told SecurityWeek, "The first two [commitments] are BS. They are pretty obvious, and I don't see anything happening about them. Similarly, the third one. I do not see the need of this Cybersecurity Tech Accord for that."

Read the rest here:
https://www.securityweek.com/cybersecurity-tech-accord-marketing-move-or-serious-security
How hackers can use artificial intelligence against us

By Chris Ciaccia, Fox News, April 25, 2018

Much has been made in recent months about the potential benefits of artificial intelligence for humanity – stopping terrorist content before it’s seen, letting people experience events they otherwise never could or performing menial tasks, such as tagging photos.

Despite all of that, artificial intelligence also has a negative side. Luminaries such as Elon Musk, the late Stephen Hawking and others have warned of a “robot apocalypse” and AI being the root cause of World War III one day in the not-too-distant future.

But what if the fear humans have for artificial intelligence isn’t robots or a sentient AI system similar to Skynet in the "Terminator" movies – but humans themselves?

Sometimes known as adversarial AI, artificial intelligence can be exploited by hackers in everyday situations, such as getting money out of an ATM, criminals sneaking across borders or taking over your smart speaker and wreaking havoc with your bank account.

"As with any new technology, hackers are going to look for a way to exploit it for their gain," Koos Lodewijkx, VP and CTO of Security Operations and Response, IBM Security said in an email to Fox News.

Lodewijkx added: "Our research sees cybercriminals being able to fool voice systems to make purchases on their behalf or even attack autonomous vehicles through stickers on stop signs to confuse them. A whole new field of research at universities and tech companies is looking at ways to defend AI systems from these sort of attacks before they become a reality."

Via research working with universities and other tech companies, IBM has spotted some of the more common ways hackers can corrupt AI systems and turn them against humanity. For example, a sticker covering a street sign that a road is closed could throw off an autonomous vehicle and cause it to not stop, whereas a human driver would know the difference.

Other examples include streaming songs on a smart speaker with one of the songs tweaked to hide audio commands a smart speaker could follow that could clean out a bank account. Another possibility involves fooling facial recognition algorithms by using smart glasses that could misidentify the hacker wearing them, something that researchers at Carnegie Mellon University did in fact create to show the downside of AI systems.

One notable example has already happened, even if the problem was caught rather quickly. In 2016, Microsoft built a Twitter bot using artificial intelligence, Tay, which was designed to mimic and converse with users in real time. However, it became corrupted and caused significant controversy when it posted racist and offensive tweets, as people took advantage of its machine learning capabilities. Tay was shut down just 16 hours after it was originally launched.

As hackers look for new ways to exploit AI systems, researchers are looking at ways to defend them before they are even attacked. IBM recently released an open-source software library to help secure AI systems. While this framework may help in the future, there is the more immediate need of what the average person can do to protect themselves now, given the prevalence of artificial intelligence in our everyday lives.

Lodewijkx suggests taking some basic precautions, similar to what we already do now with our devices, including making sure software is up-to-date and keeping an eye out for odd behavior from your devices.

Read the rest here:
Despite Risks, Nearly Half of IT Execs Don't Rethink Cybersecurity after an Attack

By Marc Wilczek, Dark Reading, April 25, 2018

A recent survey reveals a troubling degree of security inertia lurking among scores of organizations. But there are a few bright spots.

A wise person once said, "Insanity is doing the same thing over and over again and expecting different results." However, in a recent survey done by CyberArk for its Global Advanced Threat Landscape Report 2018 (registration required), almost half (46%) of 1,300 IT executives in seven countries say they rarely change their security strategy — even after a cyberattack.

The survey findings suggest that a troubling degree of security inertia lurks within scores of organizations and effectively renders them unable to repel or contain cyber threats. Such complacency puts sensitive corporate data, IT infrastructure, and assets at risk. In fact, an overwhelming 46% of respondents say their organization can't stop the bad guys from infiltrating internal networks each time they try. More than a third (36%) say that their company's administrative credentials are stored on personal computers in Word or Excel documents. Further, half (50%) of the respondents admit that their customers' privacy or personally identifiable information could be at risk because their data is not secured beyond the legal minimums.

Flexibility Overrides Security

Whether organizations use cloud computing, build large-scale data silos, or connect thousands of IoT devices, going digital inevitably means facing a whole range of new cyber threats — with safeguarding privileged accounts being the starting point, according to the study. Most IT security pros say that protecting an IT environment starts with safeguarding privileged accounts. Nine out of 10 (89%) of experts surveyed say IT infrastructure and critical data are not fully protected unless privileged accounts, credentials, and secrets are under digital lock and key. Regarding cybersecurity threats, respondents worry most about targeted phishing attacks (56%), insider threats (51%), ransomware or malware (48%), unsecured privileged accounts (42%), and unsecured data stored in the cloud (41%).

IT security respondents also say the proportion of users with local administrative privileges on their devices increased from 62% in 2016 to 87% in 2018 — a 25% jump. This seems to indicate that employee demands for flexibility are overriding best data-protection practices.

The automation that is part and parcel of the cloud and DevOps mean privileged accounts, credentials, and secrets are being created at breakneck speed. If breached, these provide attackers with an ideal platform from which they can gain access to sensitive data across networks, data and applications, or cloud infrastructure they can use for illicit cryptomining activities. More organizations are acknowledging this security risk but nevertheless adopt a lax approach to cloud security.

When it comes to the cloud, 49% of organizations surveyed have no privileged account security strategy. More than two-thirds (68%) shift the responsibility for cloud security to the vendor and the built-in security features of its cloud solution. Another 38% say their cloud provider doesn't provide adequate protection.

Reforming Security Culture

Security is often misperceived as a cost factor or necessary evil rather than a differentiating factor or competitive advantage. Consequently, banishing cybersecurity inertia will involve making it key to organizational strategy and behavior. To that end, most respondents to the survey (86%) say security should be a routine board-level discussion item, which suggests that currently there is a potentially disastrous disconnect between cybersecurity and the C-suite.

Read the rest here:
Let’s destroy Bitcoin

By Morgan Peck, MIT Technology Review, April 24, 2018

In 2009, Satoshi Nakamoto served the world an entirely new kind of currency. It was one that people could move over the internet instantaneously and nearly free of charge. Issued and distributed not by a central bank but by its own users, it drew the drapes of privacy around financial transactions while making forgery—in theory, at least—impossible.

It’s nine years later, and there are now 24 million active Bitcoin wallets in use around the world. The value of a single bitcoin has risen from about a dollar in 2011 to as high as $19,700 in late 2017.

But success, of course, breeds competition. And Bitcoin is now clearly the dominant cryptocurrency; as of this writing, in early April, its market cap was three times that of Ethereum, its nearest competitor, and roughly equal to those of all other cryptocurrencies combined.

Yet while Bitcoin has established an economy in which it’s impossible to forge transactions, it provides no defense against replication of the idea itself. No one can copy an individual bitcoin, but anyone can copy the idea of Bitcoin. So how might a government, or a corporation, or even ordinary people, go about doing so in a way that makes Bitcoin useless or redundant? Here are a few scenarios.

Option one: Government takeover

The year is two-thousand-something-big, and it’s the day your taxes are due. But you don’t file them. Instead an algorithm automatically makes a withdrawal from your electronic wallet, in a currency called Fedcoin.

It’s the digital version of those crunchy bills you only vaguely remember from many years ago, back before the central banks began taking paper cash and redeeming it for fedcoins. Over the years, you’ve seen less and less hard currency. You don’t need it anymore, not when you can walk into a local bank, verify your identity, and set up a wallet on your phone. Sure, you still have a few dollar bills. But they are tucked away as souvenirs.

This hypothetical technology—a central-bank-issued digital currency built with a tweaked version of the Bitcoin blockchain—was described by David Andolfatto, a researcher at the Federal Reserve Bank of St. Louis, and later refined by Sahil Gupta, who as an undergraduate at Yale wrote a study on how a currency like Fedcoin would work. With some colleagues, he wrote code to test a simulation.

In their system, a blockchain records transactions, just the way it happens with Bitcoin. Instead of being updated by a network of unaffiliated peers, however, the Fedcoin ledger is managed by institutions certified by the Federal Reserve. “These authorized nodes could be things like Bank of America, JP Morgan—basically, trusted institutions,” Gupta told me.

Each bank is responsible for a chunk of addresses on the blockchain. When new transactions come through, the bank validates them in a new block and sends it to the Fed. The Fed then acts as the final arbiter, checking the entries and unifying the blocks into a master version of the blockchain that it makes public.

To use fedcoins, people must first show proof of identity and set up a wallet with the Federal Reserve or an affiliate bank, at which point they can buy the new currency with US dollars at a one-to-one ratio. A scheme like this, says Gupta, might gain popularity and ultimately result in the slow disappearance of physical cash.

“I’d imagine people first get comfortable spending Fedcoin on things like groceries and movie tickets,” he says. “As people realize it’s easier than cash, as businesses realize it’s cheaper than credit cards, and as banks realize it’s literally more secure, so goes the process by which dollars are phased out of the money supply and Fedcoin phased in.”

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.

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...

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 cyber community.

Send your article ideas to Don Creamer at:

doncream@outlook.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

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

Chapter Officers:
President: Colleen Murphy
Executive Vice President: Scott Frisch
Vice President: Ernest Campos
Vice President of Membership: David Reed
• Deputy VP Membership: Melissa Absher
Vice President of Training: Mark Heinrich
• Deputy VP Training: Susan Ross
Treasurer: Mark Maluschka
• Deputy Treasurer: Vacant
Communications Officer: Anna Johnston
• Dep. Communications Officer: Vacant
Recorder/Historian: Erik Huffman
• Deputy Recorder/Historian: Vacant
Member at Large: James Asimah
Member at Large: Dawn Wellein
Member at Large: Bill Blake
Member at Large: Jim Blake
Dir. of Certification: Derek Isaacs
• Dep Dir Certifications: Kurt Danis
Dir. of Professional Outreach: Vacant
• Dep Dir. of Professional Outreach: June Shores

Committee Chairs:
Ethics: Tim Westland
IT Committee: Bill Welker
Mentorship: Melissa Absher
Recognition: Erik Huffman
Sponsorship: Ernest Campos
Transformation: Ernest Campos
Newsletter: Don Creamer

Hackers once stole a casino’s high-roller database through a thermometer in the lobby fish tank

By Oscar Williams-Grut, Business Insider, April 15, 2018

Hackers are increasingly targeting “internet of things” devices to access corporate systems, using things like CCTV cameras or air-conditioning units, according to the CEO of a cybersecurity firm.

The internet of things refers to devices hooked up to the internet, and it has expanded to include everything from household appliances to widgets in power plants.

Read the rest here:

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