ISSA™ Information Systems Security Association
The Global Voice of Information Security

Kansas City ISSA Newsletter

August 24, 2017
Federal Financial Institutions Examination Council (FFIEC) Assessment
Hereford House

Inside this issue:

Peer Networking
Education & Training
Career Opportunity and Growth
Industry Tools & Resources
Special Offers & Discounts
Insight Into Best Practices
ISSA

Volume 47, Issue 1 August 2017

The President's Corner

Hello ISSA Kansas City Members and Happy August!

Hope you all enjoyed the last presentation on "Bypassing your network security – How likely is it?" by Bryan Bailey. If you have any feedback please email me at President@kc.issa.org.

The ISSA and ESG (Enterprise Strategy Group) have joined forces again to launch the **2nd Annual Global Research Survey**, which provides the collective voice of cyber security professionals. This ground breaking research survey gained enormous media attention in 2016 because of the value placed on qualified responses from individuals who are experienced cyber security professionals – our ISSA members. Complete the survey now: https://survey.az1.qualtrics.com/jfe/form/SV_9sKCvjEOZDENmVn

ISSA International conference is October 9-11, 2017 at the Sheraton Hotel & Marina in San Diego, California. We look forward to welcoming you and over 800 of your colleagues and peers at the conference. If you have not registered yet. Please **register** early to save!

Sincerely,
Naeem Babri
President, ISSA Kansas City

Upcoming ISSA-KC Monthly Chapter Meeting Schedule

August 24, 2017 ***Federal Financial Institutions Examination Council (FFIEC) Assessment*** Integrity Hereford House	September 28, 2017 ***New Era in Endpoint Security*** Carbon Black Lidia's Italy	October 26, 2017 ***Evolve Beyond Disaster Recovery to IT Resilience*** Zerto Brio's Restaurant

ISSA KC July 2017 Chapter Meeting Recap

Bypassing your network security – How likely is it?

On July 27, 2017, the ISSA-KC Chapter members and other security professionals held a meeting at Brio's restaurant to network and attend the monthly chapter meeting, on the topic "Bypassing your network security – How likely is it?". Bryan Baily, CISSP, a security sales executive with extensive experience in network security presented. The presentation covered how likely is a breach to your network security? What's the global view of network security today? In addition Bryan showed the latest NSS Labs report on which vendors are doing the best with Zero Day threats and Malware. Please join me in congratulating Ted Combs winner of the ISSA Visa $50.00 gift card, and Ted Heiman winner of the 32 inch flatscreen television.

Security & Privacy Articles and News

U.S. senators to introduce bill to secure 'internet of things'

Author: Dustin Volz, Editing by Bill Rigby August 1, 2017
http://www.reuters.com/article/us-usa-cyber-congress-idUSKBN1AH474

(Reuters) - A bipartisan group of U.S. senators on Tuesday plans to introduce legislation seeking to address vulnerabilities in computing devices embedded in everyday objects - known in the tech industry as the "internet of things" - which experts have long warned poses a threat to global cyber security. The new bill would require vendors that provide internet-connected equipment to the U.S. government to ensure their products are patchable and conform to industry security standards. It would also prohibit vendors from supplying devices that have unchangeable passwords or possess known security vulnerabilities.

Republicans Cory Gardner and Steve Daines and Democrats Mark Warner and Ron Wyden are sponsoring the legislation, which was drafted with input from technology experts at the Atlantic Council and Harvard University. A Senate aide who helped write the bill said that companion legislation in the House was expected soon.

"We're trying to take the lightest touch possible," Warner told Reuters in an interview. He added that the legislation was intended to remedy an "obvious market failure" that has left device manufacturers with little incentive to build with security in mind.

The legislation would allow federal agencies to ask the U.S. Office of Management and Budget for permission to buy some non-compliant devices if other controls, such as network segmentation, are in place. It would also expand legal protections for cyber researchers working in "good faith" to hack equipment to find vulnerabilities so manufacturers can patch previously unknown flaws.

Security researchers have long said that the ballooning array of online devices including cars, household appliances, speakers and medical equipment are not adequately protected from hackers who might attempt to steal personal information or launch sophisticated cyber-attacks.

Between 20 billion and 30 billion devices are expected to be connected to the internet by 2020, researchers estimate, with a large percentage of them insecure. Though security for the internet of things has been a known problem for years, some manufacturers say they are not well equipped to produce cyber secure devices. Hundreds of thousands of insecure webcams, digital records and other everyday devices were hijacked last October to support a major attack on internet infrastructure that temporarily knocked some web services offline, including Twitter, PayPal and Spotify.

The new legislation includes "reasonable security recommendations" that would be important to improve protection of federal government networks, said Ray O'Farrell, chief technology officer at cloud computing firm VMware.

GOVERNMENT IT REPORT
New Cybersecurity Policy Will Impact Federal IT Market

Print Email
By John K. Higgins • E-Commerce Times • ECT News Network
Jul 24, 2017

Federal agencies already under the gun to modernize their information technology capabilities have a new set of standards to meet as a result of an executive order President Donald Trump issued this spring. The directive not only will affect agency managers in their IT operations and acquisition activities, but also will have a significant effect on IT vendors.

The Trump initiative "adds another important piece to the U.S. federal IT modernization puzzle," said Katell Thielemann, research vice president at Gartner. "Various parts of the executive order will have a direct impact on the U.S. federal market," she wrote in an 18-page briefing on the program. A key element of the order is that responsibility for cyberprotection has been elevated to the level of cabinet officers and the heads of various agencies rather than residing with their IT or cybersecurity officers. "The President will hold heads of executive departments and agencies accountable for managing cybersecurity risk to their enterprises," reads the executive order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," issued on May 11.

Agency heads will be held accountable to the president "for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data," it states.

Call for Swift Action
The order requires agencies to comply "immediately" with several specific mandates:

• Each agency shall use the "Framework for Improving Critical Infrastructure Cybersecurity" developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk. The framework was developed by NIST generally for private sector use and has been widely adopted not only by critical infrastructure companies but also by a wide range of businesses.

• Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud and cybersecurity services.

Agencies must deliver a report by early August on their cyber-risk mitigation and acceptance choices, as well as their plans to implement the NIST framework. After reviewing the reports, the Department of Homeland Security and the Office of Management and Budget must submit a joint plan for the cyberprotection of the executive branch enterprise by early October. The emphasis on "executive branch enterprise" is a clear statement of policy that cybersecurity protection now is considered a government-wide goal, versus isolated agency efforts.

The executive order also links cyber protection to the goal of moving faster to modernize federal IT operations in general.

"Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture," says the executive order. To advance IT performance, the order requires the director of the American Technology Council to provide a report to the president, also by early August, "regarding modernization of federal IT." The White House established the ATC prior to issuance of the executive order to "coordinate the vision, strategy, and direction for the federal government's use of information technology and the delivery of services through information technology."

As a follow-up to creating the ATC, President Trump met with 18 tech industry leaders last month. While the order embodies many new and upgraded standards, the overall goal represents significant continuity with prior efforts, and builds upon Obama administration policies "rather than deviating sharply," DLA Piper attorneys Sydney M. White and Jim Halpert note in an online post.

Marketing Modifications

Still, the Trump initiative will require IT providers to significantly adjust their marketing efforts. For example, vendors should "clearly articulate ... risk management positioning and governance enabling solutions," along with "targeting the main groups of federal stakeholders," Gartner's Thielemann advised, including "influencers, procurers, enterprise agency end users and mission agency end users." IT providers who support the federal enterprise IT environment should "lead an assessment of ... offerings through a cloud-based digital platforms lens," she suggested. Vendors should evaluate "the implications of emerging enterprise shared services moving to centralized digital platforms," Thielemann recommended.

Vendors may have to make more investments to enhance their offerings to meet the upgraded goals, although "IT vendors already have to make investments they would not normally have to make elsewhere" in order to pursue the federal market, Thielemann noted. "These investments are not for the faint of heart, so IT vendors are making continual strategic trade-offs with regard to the level of investments they are willing to make," she told the E-Commerce Times. Such investing is a continuous process among contractors already in the market, noted John Slye, research analyst at Deltek.

"Most experienced vendors and service providers are aware and have been addressing these concerns out of necessity, and anything that adds rigor and review to services or products adds effort and cost," he told the E-Commerce Times. However, companies new to the federal market may need to put more into product development efforts for government customers.

The reports required by the directive, "coupled with additional action from NIST, could lead to additional requirements on government contractors," suggests an analysis by Eric Crusius and Norma Krayem at law firm Holland and Knight. "Certainly, the emphasis on shared services could further direct changes to how the government obtains IT services from contractors and a focus on federal IT modernization provides a series of opportunities for contractors as well," they wrote.

Providers who specialize in exclusively offering cyberprotection products and services are in a good position to benefit from the Trump policies and many already have, Thielemann reported. The Trump initiatives on cybersecurity and associated IT modernization are in line with recent federal agency moves that recognize that standard government practices actually may hinder timely acquisition of cybersecurity offerings, she noted. "Several federal organizations have also realized that the unique federal rules of engagement when it comes to market positioning and procurement approaches can be a deterrent for cybersecurity vendors with commercial pedigrees. They are responding by looking for ways to attract them to the market faster," Thielemann said.

Special Programs and Cloud IT

The Defense Innovation Unit Experimental program (DIUx) has been created to serve as a bridge between Defense Department components confronting major security challenges and private sector companies at the cutting edge of technology. DIUx offices have been established in California's Silicon Valley, Boston and Austin, Texas, to promote dialog with the private sector. In addition, the General Services Administration has set up Special Item Numbers, or SINs, for cybersecurity products to accelerate acquisition, Thielemann noted.

The Trump cybersecurity initiative likely will spark a much greater degree of interest in shared services, for which cloud technology is the most visible vehicle.

"The linking of shared services with modernization is opening the route to cloud-based government digital platforms," Thielemann said, noting the commitments of major players such as Amazon Web Services and Microsoft in the federal market. "This cybersecurity aspect has been a theme that has evolved in parallel with agency efforts to achieve efficiencies and increase the effectiveness of their IT infrastructure and applications through cloud, and so forth. A few years ago, one question with the feasibility of the cloud was whether it could be secure," said Deltek's Slye. "Now we are hearing how cloud is an avenue to vastly improve security," he continued. "It comes down to the implementation and how cloud services have matured. The cost, complexity, and time it takes to modernize many legacy systems makes placing those systems in a cloud environment with a security layer in front of it an appealing option. So security has become a 'selling point.' for many cloud advocates.

WannaCry Hero Charged With Creating $7,000 Banking Malware
Thomas Fox-Brewster, Forbes Staff, August 3, 2017
https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacry-killswitch-hero-arrested/#1585f5a54222

In an astonishing turn of events, the man who stopped the spread of the WannaCry ransomware earlier this year has been arrested and charged with creating a banking malware known as Kronos.

Marcus Hutchins, also known as MalwareTech, was held in Nevada, just as he was getting ready to head home from the Las Vegas-based hacker conferences Black Hat and Def Con. News of his apprehension came first via Motherboard.

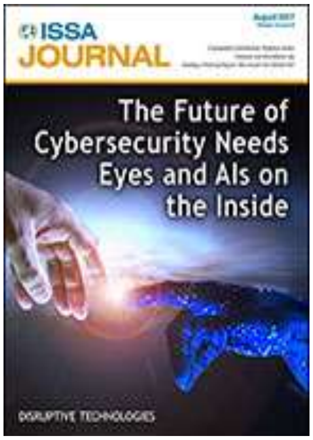
The 23-year-old was hailed as a hero for registering a web domain the ransomware creators planned to use, which turned out to be a killswitch, preventing the NSA cyberweapon-powered malware from spreading further. Just before his arrest he was attending the Black Hat and Def Con hacker conferences in Las Vegas. His most recent tweets, from 24 hours ago, indicated he was getting ready to board a flight.

But now his reputation is under threat as he was charged as one of two people responsible for running the Kronos malware. The software first emerged in 2014, attempting to pilfer individuals' banking logins, selling on Russian criminal markets for as much as $7,000, according to IBM research. It was later altered to infect point-of-sale systems too. According to the short indictment released today, Hutchins was responsible for updating and spreading the malware alongside an unnamed co-conspirator. Intriguingly, prosecutors alleged the unnamed party sold the tool on AlphaBay, a dark market that law enforcement recently took over and shut down. Hutchins, whose day job is researching malware, tweeted in July 2014 asking for a sample of Kronos. He is, as the Department of Justice noted in its press release, innocent until proven guilty.

According to that release, the government saw the Kelihos botnet spread Kronos. That's another malware that Hutchins has previously researched and published on, as recently as April this year. The Electronic Frontier Foundation (EFF) said it was trying to get in touch with Hutchins too. The EFF has provided legal assistance to hackers facing legal threats in the U.S. before. According to Mabbitt, Hutchins doesn't have legal representation and will need funds to get a lawyer. The U.K. National Crime Agency told Forbes it was aware of the reports, but said it was a matter for the FBI.

News of Hutchins arrest landed on the same day that funds from the WannaCry wallets used to collect ransoms started moving, as the criminals behind the enterprise started shifting bitcoin to anonymizing currency Monero. Hutchins was notoriously hounded by British press in the days after he took WannaCry down. He told Forbes he didn't want his real identity revealed and was concerned about the WannaCry criminals coming after him now his name and whereabouts were known.

ISSA Journal, August, 2017


ISSA JOURNAL
The Future of Cybersecurity Needs Eyes and AIs on the Inside
DISRUPTIVE TECHNOLOGIES

August 2017

Volume 15 - Issue 8

Feature articles include:

- The Future of Cybersecurity Needs Eyes and AIs on the Inside - Jason Kichen
- Battening Down for the Rising Tide of IoT Risks - Anthony J. Ferrante
- Blockchain: Considerations for Infosec - Gerry McGreevy
- When You Cannot Be Silent: Whistle-Blowing 2.0 - Avani Desai
- Disrupting the Disruptors: How Cybersecurity Can Confront Hackers and a Skilled Worker Shortage with Its Own Disruptive Technologies - Tyson Macaulay

Members: please click on the following Journal issue links for access:
Computer: Bluetoad - PDF; Mobile: ePub - Mobi

Not a member? Read this month's feature article - The Future of Cybersecurity Needs Eyes and AIs on the Inside - at no charge or Join Now and gain full access to the *ISSA Journal*.

Certification Corner

CISSP Study Group

What is the CISSP®? (Certified Information Systems Security Professional)

The vendor-neutral CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks.

Subject: CISSP Study Group
Where: Looking for a New Location
When: Monday’s, starting September 11th through October 8, 2017.

* More information to come on the logistics

Contact: Mark Waugh, ISSA Education Committee Member
waugh.mark.r@gmail.com
913-636-7900

Director of Education, Larry Dilley
certification@kc.issa.org

Webinars/Conferences

DATA CONNECTORS
SECURING YOUR FUTURE
DATA CONNECTORS IT SEC CONFERENCES
Kansas City | September 21
#DCKC

The Kansas City IT Security Conference is coming on September 21st.

Join us at the event to:

- Connect and collaborate with industry leading professionals
- Earn CPE Credits
- Experience a diverse learning environment
- Gain insider knowledge on recent trends
- Learn how industry professionals are implementing and improving their processes

REGISTER HERE VIEW AGENDA

8:15a.m. - 5:00p.m.

DoubleTree by Hilton Kansas City - Overland Park
10100 College Blvd.
Overland Park, KS 66210

Join us **October 9-11, 2017** at the **Sheraton Hotel & Marina in San Diego, California** for solution oriented, proactive and innovative sessions focused on the ***Digital Danger Zone***.

Each day, cyber threats become increasingly intricate and difficult to detect. Over the past year, we saw that with the rise of device connectivity came boundless opportunities for malicious hackers to attack device vulnerabilities. No cyber security professional can become an expert on these digital dangers without continued efforts to educate themselves on the industry's latest trends and technologies.

We look forward to welcoming you and over 800 of your colleagues and peers in San Diego as we discuss topics ranging from incident response to application security to business skills for the information security professional. Join us at the 2017 ISSA International Conference and we'll help you navigate the *Digital Danger Zone*.

Detailed Schedule

Click here for session descriptions

Register Now

ISSA-Kansas City August Chapter Event

August 24, 2017 ISSA Chapter Meeting

Speaker: David A. Nelson, Jr., CISSP

Bio: Dave is a Certified Information Systems Security Professional (CISSP) with 20 years of experience and a Fellow with the Information Systems Security Association (ISSA). He has lead technology organizations in both the public and private sector. Prior to founding Integrity, he most recently was the Chief Information Security Officer for a leading health informatics company. He also managed an information security group for a top 5 U.S. banking organization, was the CIO for a higher education institution and served as the information security officer for one of the largest municipal governments on the east coast.

Dave received his Bachelor of Science degree with a major in Computer Information Systems from Excelsior College. He has also taught and developed information technology curriculum at the post-secondary level. Dave is a published author and speaker at national conferences. He lives in the Des Moines, IA area with his wife and 4 children.

Topic: Using the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool: A Guide for Financial Institutions
Topic Summary: As the cybersecurity threat to financial institutions continues to grow, the FFIEC has released the Cybersecurity Assessment Tool to help institutions understand and rate their risk levels. This session will cover the basics of the tool, who should use it and how it can help institutions address cyber risk. We'll also discuss what the tool will not do and what institutions need to do to fill in the gaps.

Location: Hereford House, Town Center Plaza, 5001 Town Center Drive, Leawood, KS. 66211

Agenda:
11:30 AM - 12:00 PM Greeting and registration
12:00 PM - 1:00 PM - Meeting & Presentation
1:00 PM - 1:30 PM - Questions, Answers & Networking

Menu:
Lunch : Choice of one: Beef, Chicken, or Salmon,
Salad, Potato, Vegetable, Drink

Soft drinks, Iced Tea, Coffee

*Vegetarian option available, please note at registration at Brio
* *Menu subject to change. **

Price:
$20.00 for ISSA Members,
$30.00 for Guests/Non-Members
Maximum Reservation: 35
Credit(s): 1 CPE credit

We look forward to seeing you at the event. If you have any questions about the event or how to register, please email our RSVP email, or contact the venue for directions.

*** Register ***

The Information Systems Security Association (ISSA) is an international organization providing educational forums, publications and peer interaction opportunities that enhance the knowledge, skills and professionalism. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

novacoast

OPTIV

IBM

radware

AOS

CARBON BLACK
ARM YOUR ENDPOINTS

InteliSecure

Integrity
SECURITY | RISK | COMPLIANCE

VARONIS

tenable network security

cisco
OpenDNS

viawest

DELL

SonicWALL | One Identity

Lockpath

netskope

President
Naeem Babri
president@kc.issa.org

Vice President
Cheryl Cooper
mailto:vp@kc.issa.org

Director of Social Media
Melissa Salazar
socialmedia@kc.issa.org

Secretary of Board
Rochelle Boyd
secretary@kc.issa.org

Newsletter Chief Editor
Cheryl Cooper
newsletter@kc.issa.org

Treasurer
Gary Kretzer
treasurer@kc.issa.org

Director of Membership
Wei Cheng
membership@kc.issa.org

Director of Education
Larry Dilley
certification@kc.issa.org

Director of Programs
Carmen Banks
programs@kc.issa.org

Webmaster
Thomas Badgett
webmaster@kc.issa.org

Director of Events
Dan Boeth
events@kc.issa.org

Study Group coordinator
Mark Waugh
issakc-study@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney