Information Systems Security Association
The Global Voice of Information Security

Kansas City ISSA Newsletter

Volume 49, Issue 1 October 2017

October 26, 2017

Evolve Beyond Disaster Recovery to IT Resilience

Brio's Restaurant

Inside this issue:

The President's Corner

Hello ISSA Kansas City Members!

Hope you call enjoyed the last presentation on "New Era in End Point Security" by Rick Perkins. Do share your feedback on the September meeting. I am looking forward to seeing most of you during ISSA KC November Happy Hour at La Bodega.

Please let us know if you would like to volunteer as an ISSA KC Board or committee member for 2018, email me at, president@kc.issa.org. Also check out ISSA's Special Interest groups for particular topics, like Security Awareness, Women in Security, Healthcare and Financial.

Thank for submitting your ISSA KC bi-yearly Survey!

Sincerely,

Naeem Babri

President, ISSA Kansas City

facebook LinkedIn twitter

Upcoming ISSA-KC Monthly Chapter Meeting Schedule

October 26, 2017	November 9, 2017	December 7, 2017
Evolve Beyond Disaster Recovery to IT Resilience	**ISSA HAPPY HOUR**	Combined meeting with ISACA
Brio's Restaurant	La Bodega, Leawood, KS	

ISSA KC September 2017 Chapter Meeting Recap

New Era in End Point Security

On September 28, 2017, the ISSA-KC Chapter members and other security professionals held a meeting at Lidia's Italy restaurant to network and attend the monthly chapter meeting, on the topic "Era in End Point Security". Rich Perkins, presented and discussed the current state of endpoint security and how we need to change our way of thinking in order to get ahead of the attackers. We had 26 attendees and several gift giveaways, Echo Speakers went to three members, the $50.00 Visa gift card went to Brian Connell, and Adam Schlicht won a dinner for two from Lidia's restaurant. Congratulations to the winners!

Congratulations to Brian Connell

Winner of the $50.00 Visa Gif Card!

National Cyber Security Awareness Month Resources

October is National Cyber Security Awareness Month (NCSAM), a time to focus on how cybersecurity is a shared responsibility that affects all Americans. NCSAM is a collaborative effort between the U.S. Department of Homeland Security (DHS) and its public and private partners, including the National Cyber Security Alliance, to raise awareness about the importance of cybersecurity and individual cyber hygiene. The following materials are from past DHS National Cyber Security Awareness Months to give you an idea of what to expect this coming October. We encourage you to use these resources as a reference to promote your organization's involvement in raising cybersecurity awareness.

To receive cybersecurity tips year round, please visit the Stop.Think.Connect.™ Campaign and become a *Friend* of the Campaign. The Stop.Think.Connect. Toolkit is filled with tips, fact sheets, and shareable resources: www.dhs.gov/stopthinkconnect-toolkit.

BEST PRACTICES FOR USING PUBLIC WI-FI

Public Wi-Fi networks can now be found almost everywhere – in airports, coffee shops, libraries, restaurants, malls, and hotels – making it easy for anyone to connect to the Internet wherever they are. Although these Wi-Fi hotspots can be convenient, they are not always secure, potentially exposing you to online risks and presenting an opportunity for cybercriminals to steal sensitive information. It is important to understand these risks and take measures to protect yourself while connecting to Wi-Fi networks.

SIMPLE TIPS

- **Think before you connect.** Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, or café – be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate. Cybercriminals can easily create a similarly named network hoping that users will overlook which network is the legitimate one. Additionally, most hotspots are not secure and do not encrypt the information you send over the Internet, leaving it vulnerable to cybercriminals.
- **Use your mobile network connection.** Your own mobile network connection, also known as your wireless hotspot, is generally more secure than using a public wireless network. Use this feature if you have it included in your mobile plan.
- **Avoid conducting sensitive activities through public networks.** Avoid online shopping, banking, and sensitive work that requires passwords or credit card information while using public Wi-Fi.
- **Keep software up to date.** Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent cybercriminals from being able to take advantage of known vulnerabilities.
- **Use strong passwords.** Use different passwords for different accounts and devices. Do not choose options that allow your device to remember your passwords. Although it's convenient to store the password, that potentially allows cybercriminals into your accounts if your device is lost or stolen.

Bill Would Require Pentagon to Assess Security Risks to Electric Grid

By Morgan Chalfant with The Hill, September 29, 2017

http://thehill.com/policy/cybersecurity/353109-bill-would-require-pentagon-to-assess-security-risks-to-electric-grid

A bill introduced by a bipartisan group of House lawmakers this week would require the Pentagon to report to Congress on significant security risks to the U.S. electric grid and their impact on the U.S. military.

The bill would require the Pentagon, in coordination with the Energy Department, Homeland Security Department and the director of national intelligence, to issue a report identifying "significant security risks" that malicious cyber actors pose to critical defense electric infrastructure, and the potential effect of those threats on the U.S. armed forces.

The report would also have to assess the benefits and challenges of isolating U.S. military infrastructure from the electric grid. Finally, the Pentagon would be required to recommend measures to mitigate these security risks.

The legislation was introduced by Rep. Jacky Rosen (D-Nev.) and is cosponsored by Reps. Elise Stefanik (R-N.Y.), Brian Fitzpatrick (R-Pa.) and Dan Lipinski (D-Ill.).

"I'm proud to work across the aisle to introduce this legislation that will help ensure America's military readiness by requiring top officials to identify and report any vulnerabilities that might jeopardize our core defense missions," said Rosen, who is a member of the House Armed Services Committee.

"In this day and age, with adversaries around the globe developing their cyber capabilities, we must redouble our efforts to protect against these sorts of attacks," Stefanik, who chairs the subcommittee with oversight of the Pentagon's cyber capabilities, said in a statement.

"This legislation will help Congress and our military gain a better understanding of the vulnerabilities and dependencies of these systems in order to better protect our homeland, and I encourage my colleagues to support this effort," Stefanik said.

Lipinski emphasized that the bill will help guard the electric grid "from attacks by America's enemies who are trying to take down our defenses" as well as harden the entire grid against cyberattacks that threaten to disrupt American lives and U.S. business operations.

DHS Bans Kaspersky Products from Federal Agency Computers

The Department of Homeland Security, citing potential vulnerabilities, ordered executive branch agencies to remove products provided by the Russian-owned company.

By Alan Neuhauser, U.S. News Staff Writer, Sept. 13, 2017

https://www.usnews.com/news/national-news/articles/2017-09-13/dhs-bans-kaspersky-cybersecurity-software-from-federal-agencies

A Kaspersky employee demonstrates company products at a cybersecurity conference in France in January. The firm has come under intense scrutiny for its ties to the Kremlin. Raphael Satter/AP

The Department of Homeland Security on Wednesday ordered all federal executive branch agencies to stop using products provided by the Russian-based cybersecurity firm AO Kaspersky Lab.

Acting DHS Secretary Elaine Duke issued the directive, warning of "information security risks" presented by Kaspersky anti-virus products and other software, which "provide broad access to files" and "can be exploited by malicious cyber actors to compromise" federal computer systems, the order said.

"The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks," DHS said in its order. "The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security."

Agencies will have 90 days to remove Kaspersky products from their systems. Kaspersky makes some of the most popular anti-virus and cybersecurity software in the world. However, cybersecurity experts have warned for years about the risks posed by the Moscow-based company due to its apparent close ties to the Kremlin. As early as 2015, Bloomberg News reported that the company has "close ties to Russian spies."

Scrutiny of the company mounted in 2017, fueled by U.S. intelligence assessments and high-profile federal investigations of Russian interference in the 2016 election. This summer the General Service Administration, which oversees purchasing by the federal government, removed Kaspersky from its list of approved vendors.

Kaspersky, in a statement, maintained that it "doesn't have inappropriate ties with any government, which is why no credible evidence has been presented publicly by anyone or any organization to back up the false allegations made against the company. The only conclusion seems to be that Kaspersky Lab, a private company, is caught in the middle of a geopolitical fight, and it's being treated unfairly even though the company has never helped, nor will help, any government in the world with its cyber espionage or offensive cyber efforts."

It added: "Kaspersky Lab has always acknowledged that it provides appropriate products and services to governments around the world to protect those organizations from cyber threats, but it does not have unethical ties or affiliations with any government, including Russia," the firm said. DHS, in its directive, noted that while the ban on Kaspersky "involves products of a Russian-owned and operated company," it will "take appropriate action related to the products of any company that present a security risk."

6 Places Never to Use a Debit Card

By Sid Kirchheimer, AARP Fraud Watch, September 13, 2017
https://aarpfraudwatch.yahoo.com/6-places-never-to-use-a-debit-card-165201656.html

Credit or debit? Although both cards look the same, they offer different protections.

Under federal law, if your credit card is used to make unauthorized charges after it is lost or stolen, you're liable for only $50—no matter the amount and with no time restrictions to report the fraud. And many issuers won't even charge the $50 for valued customers.

But with a debit card, you have just two business days to report an unauthorized loss or money transfer, or you could be liable for up to $500. Wait more than 60 calendar days after your statement is mailed and you could be responsible for all money pilfered from its connected account.

Although debit cards offer no-interest savings—which may factor for some plastic users– there are six places where you should never use them.

Gas stations. In addition to ATM machines, gas pumps are a popular target for "skimming," in which crooks place a portable card-reading device inside the pump. When a motorist inserts a debit card and enters the required personal identification number, the hidden device (which can be purchased on the Internet for less than $100) captures both the data from the card's magnetic stripe and the PIN. Later, the device is retrieved, and the stolen data is used to create a duplicate card to raid the victim's bank account.

Why gas stations? With only a handful of manufacturers of gas pumps, one key in the hands of a thief who gets a job at one station can be used to open pumps and install other skimmers elsewhere, especially at night or when unattended. And with older pumps, PINs may not be encrypted. If you must use a debit card (and it has a Visa or MasterCard logo versus being a cash-withdrawal-only card), choose the "credit" screen prompt, instead of "debit," so you don't have to enter your PIN. This way, the purchase amount will still be deducted directly from your bank account, but it's processed through a credit card network, providing greater protection if fraud occurs.

Online purchases. Along with providing added security should the retailer fall victim to a data breach—a hacker can't overdraft your bank account with a credit card—*most* credit cards (versus *some* debit cards) offer extra protection perks. If you don't receive the merchandise, it's defective or the wrong item, and the vendor won't issue a refund, it's easier to dispute charges with a credit card.

Many credit cards also offer extended product warranties (usually for one year beyond what's offered by the manufacturer), and some provide price protection up to 90 days, issuing you the difference if the identical item is sold for a lower price than you paid. Although certain debit cards offer these protections, the hassle factor can be greater.

Big-ticket items. Rewards aside, the above-mentioned credit card perks are especially useful for expensive products, whether purchased in store or online.

Restaurants. Eateries are among the few places where a payment card can leave your sight, and crooked waiters can—and sometimes do—disappear to write down its number for possible identity theft. Even without a PIN, someone can use your card number to make fraudulent purchases online. And restaurants without sit-down service can pose a threat, since some (along with other businesses) keep customer payment information on file but may not safeguard it.

Retail stores. Retail stores are subject to cyberattacks using sophisticated malware that specifically targets point of sale (POS) systems such as cash registers and card-swiping devices. It was this "memory-parsing" malicious software (also known as a "RAM scraper") that was behind the well-publicized hacking of payment card information of some 110 million Target customers over the 2013 Christmas season—and responsible for nearly two dozen other attacks the following year.

True, credit cards are also vulnerable in such POS attacks. But with more protections, credit card issuers always eat those losses (minus a possible $50 cap) should your plastic be hacked. Depending on when you learn of and report fraudulent use of hacked debit card data, you could be on the hook from unauthorized activity.

When a deposit is required. Risk of identity theft aside, credit cards are a wiser choice for transactions in which the final bill is uncertain—e.g., hotels, rental cars or even tools rented from a home improvement center. Reason: With a debit card, a "hold" can be placed on your account that may be greater than the expected bill, such as for hotel incidentals, including room service, or for a predicted failure to return a rental car without a full tank of gas. If this occurs, you could be denied access to the additional hold amount from your bank account until the final bill is tallied. With a credit card, hold amounts may initially appear as a pending charge until your final bill is paid, so it may not be debited until the final bill is paid. Gas stations also place holds on debit charges, which is another reason to use credit cards.

ISSA Journal October 2017

October 2017
Volume 15 - Issue 10

Feature articles include:

- Addressing Malware with Cybersecurity Awareness - Carlos Valiente, Jr.
- Malware in 2017: The More Things Change - Jacob Ansari
- Hollywood Presbyterian Medical Center Ransomware: A Retrospective Review - Steve Giles and Brian Toevs
- WannaCry/NotPetya and How We Failed Miserably! - Duncan McAlynn
- What You Don't Know Is Limiting Your Potential for Success - Gordon Merrill

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 - Addressing Malware with Cybersecurity Awareness - at no charge or Join Now and gain full access to the *ISSA Journal*.

Certification Corner

Contact: Mark Waugh, ISSA Education Committee Member For CISSP, 913-636-7900
Director of Education, Larry Dilley, certification@kc.issa.org

Webinars/Conferences

Gartner

Determine the Right Approach to Public Cloud-based Disaster Recovery

ISSA-Kansas City October Chapter Event

Discussion Topics:

- Public cloud provider DR and replication capabilities
- Third-party DR solutions that support on-premises to public cloud failover
- Benefits and challenges of different deployment approaches

Many organizations are evaluating IaaS public clouds as disaster recovery locations instead of building or using an existing secondary data center. We'll examine deployment approaches for leveraging Amazon Web Services (AWS) or Microsoft Azure for disaster recovery.

Hosted by:

Lowell Shulman, Research Director

Register

October 26, 2017 ISSA Chapter Meeting

Topic: Evolve Beyond Disaster Recovery to IT Resilience

Topic Summary: IT resilience is achieved when a company is capable of responding to a disruption so quickly that end-users and customers are not aware that a disruption occurred. Organizations that embrace this concept, which is essentially a more proactive approach to BC/DR, focus on continuous availability rather than recovery after the fact. Automation and simplification of replication and recovery are part of resilience, and ensure that companies can prove the availability of their applications and data at any time.

In this presentation learn how Zerto work towards a complete solution with no dependencies on hypervisors, hardware, or clouds in order to achieve IT Resilience.

Speaker: Kelly Lipprand

Bio Highlights: Kelly Lipprand is a Systems Engineer for Zerto supporting Kansas, Missouri and Nebraska. He has worked in high-tech and IT for over 15 years. He has extensive experience in designing and deploying converged infrastructure for public. private and hybrid cloud as well as VMware and Microsoft operating systems and software. He holds current Cisco and VMware certifications. Kelly has also directed deployment of Data Center infrastructure and circuits for multiple regional locations. He has spoken publicly, nationally and internationally at large trade shows and film festivals on many different subjects. Kelly is a foodie and loves to travel. He currently resides in Kansas City with his wife. He can be reached at kelly.lipprand@zerto.com.

Location: BRIO Tuscan Grille, Country Club Plaza, 502 Nichols Rd, Kansas City, MO 64112

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:
Salad
Choice of Chicken, Salmon or Pasta
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.

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 Boethe
events@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney