Hello ISSA Kansas City Members and Happy July!

Hope you all enjoyed the last presentation on “Email Authentication with DEMAR” by Chris Caleb. If you have any feedback please email me at President@kc.issa.org.

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!

If you currently hold certifications, you can earn CPE credits by attending chapter meetings, ISSA Web Conferences, reading or contributing an article to the ISSA Journal or volunteering for activities associated with putting on educational meetings or conferences.

Do you know ISSA members get 20% off on MindEdge Learning as member benefits? Use the code of ISSA during checkout to receive the 20% discount on the courses.

Sincerely,
Naeem Babri
President, ISSA Kansas City

Upcoming ISSA-KC Monthly Chapter Meeting Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 27, 2017</td>
<td>Bypassing your network security – how likely is it?</td>
<td>Force Point</td>
</tr>
<tr>
<td>August 24, 2017</td>
<td>Federal Financial Institutions Examination Council (FFIEC) Assessment</td>
<td>Integrity</td>
</tr>
<tr>
<td>September 28, 2017</td>
<td>More to Come</td>
<td>Carbon Black</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lidia’s Italy</td>
</tr>
</tbody>
</table>
Making a Jump to Risk Management

On Jun 22, 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 Email Authentication with DMARC. Caleb Christopher, the Director of Technical Operations at information security and risk management firm, Cino Security Solutions Ltd. and Director of Information Technology at Challenger Sports presented. The presentation covered SPF, DKIM, and DMARC records (public DNS) that help domain owners whitelist authorized senders, and allow them to specify what to do with emails that don't authenticate properly, as well as provide reporting on all emails sent on their behalf. Attendees came away with a clear understanding of the importance of email authentication to prevent spoofed/fraudulent emails (protecting domain reputation), and they came away with understanding the importance of reducing/preventing phishing certain phishing attacks.

Petya Ransomware Sinks Global Businesses into Chaos


A new ransomware exploit dubbed "Petya" struck major companies and infrastructure sites this week, following last month's WannaCry ransomware attack, which wreaked havoc on more than 300,000 computers across the globe. Petya is believed to be linked to the same set of hacking tools as WannaCry.

Petya already has taken thousands of computers hostage, impacting companies and installations ranging from Ukraine to the U.S. to India. It has impacted a Ukrainian international airport, and multinational shipping, legal and advertising firms. It has led to the shutdown of radiation monitoring systems at the Chernobyl nuclear facility.

Europol, the international law enforcement agency, could not provide operational details on the attack, spokesperson Tine Hollevoet told the E-Commerce Times, but it was trying to "get a full picture of the attack" from its industry and law enforcement partners.
Petya “is a demonstration of how cybercrime evolves at scale and, once again, a reminder to business of the importance of taking responsible cybersecurity measures,” Europol Executive Director Rob Wainwright said in a Wednesday update.

Unlike Wannacry, the Petya attack does not include any type of 'kill switch,' according to Europol. A new ransomware exploit dubbed "Petya" struck major companies and infrastructure sites this week, following last month's WannaCry ransomware attack, which wreaked havoc on more than 300,000 computers across the globe. Petya is believed to be linked to the same set of hacking tools as WannaCry. Petya already has taken thousands of computers hostage, impacting companies and installations ranging from Ukraine to the U.S. to India. It has impacted a Ukrainian international airport, and multinational shipping, legal and advertising firms. It has led to the shutdown of radiation monitoring systems at the Chernobyl nuclear facility.

Europol, the international law enforcement agency, could not provide operational details on the attack, spokesperson Tine Hollevoet told the E-Commerce Times, but it was trying to "get a full picture of the attack" from its industry and law enforcement partners. Petya "is a demonstration of how cybercrime evolves at scale and, once again, a reminder to business of the importance of taking responsible cybersecurity measures,” Europol Executive Director Rob Wainwright said in a Wednesday update. Unlike Wannacry, the Petya attack does not include any type of 'kill switch,' according to Europol.

**Variant Characteristics**
The U.S. Computer Emergency Readiness Team on Tuesday began fielding numerous reports about the Petya ransomware infecting computers around the world, and noted that this particular variant encrypts the master boot records of Windows computers and exploits vulnerabilities in the Server Message Block. The RANSOM_PETYA.SMA variant uses as infection vectors both the EternalBlue exploit, which was used in the WannaCry attack, and the PsExec tool, which is a Microsoft utility used to run processes using remote access, according to Trend Micro. Users should apply the MS17-010 security patch, disable TCP port 445, and restrict accounts with administrator group access, the firm recommended. The Petya variant uses the rundll32.exe process to run itself, and encryption is carried out using perfc.dat, a file located in the Windows folder, Trend Micro said.

The ransomware adds a scheduled task and reboots the computer system after one hour. The Master Boot record is modified, allowing encryption to take place, and a ransom note is displayed with a fake CHKDSK notice. The Petya exploit uses a hardcoded bitcoin address, making decryption more labor-intensive than it was during the WannaCry attack. However, users similarly are asked to pay US$300 to release the data. An estimated $7,500 had been paid as of Tuesday, Trend Micro estimated. However, that number could change as the attacks spread. Many companies failed to upgrade their computer systems properly following the WannaCry attack, said Gaurav Kumar, CTO at RedLock. WannaCry exploited legacy Windows systems that had not been patched, even though Microsoft issued an update in March, he told the E-Commerce Times. Governments should mount coordinated efforts to fight cyberattacks, according to Access Now, an advocate for digital rights and privacy.

The Petya attack's use of the EternalBlue exploit shows that government agencies should not be stockpiling vulnerabilities, the group argued, as the exploit has been linked to the Shadow Brokers' leak of an exploit created by the National Security Agency. "Governments should promote patching by developing and codifying vulnerabilities equities processes and through support of coordinated disclosure programs," said Drew Mitnick, policy counsel at Access Now.

**Corporations Caught**
Pharmaceutical giant Merck & Co. on Tuesday confirmed that its computer network was compromised by the attack, and said it was investigating the matter. International law firm DLA Piper confirmed that its advanced warning systems detected suspicious activity that apparently was linked to a new variant of the Petya malware. The firm said it had taken down its systems to prevent the spread, and that it had enlisted forensic experts and was cooperating with FBI and UK National Crime Agency investigators. Advertising and public relations firm WPP said it was working with its IT partners and law enforcement agencies to take precautionary measures, restore services where they have been disrupted, and keep the impact on clients, partners and people to a minimum. The company has taken steps to contain the attack and is working to return to normal operations as soon as possible, while protecting its systems. International shipping firm A.P.
Moeller-Maersk reported that a number of company IT systems were down following the attack and said that it had shut down a number of systems to contain the problem. APM terminals were down in a number of ports, and the Port Authority of New York and N.J. issued a warning to delay arrivals in light of APM’s system issues.

“Is there a difference between cybersecurity and information security?”

Not only is this a great question, but it’s something we’ve heard many times before. Cybersecurity and information security are so closely linked that they’re often thought of as synonymous. But, there are some important distinctions between the two. Below, we’ll explain those distinctions, review a couple important areas of overlap, and discuss why this differentiation—and the evolution of these definitions—matters in the security sector.

INFORMATION SECURITY
Information security (or “InfoSec”) is another way of saying “data security.” So if you are an information security specialist, your concern is for the confidentiality, integrity, and availability of your data. (This is often referred to as the “CIA.”) Most modern business data resides electronically on servers, desktops, laptops, or somewhere on the internet—but a decade ago, before all confidential information migrated online, it was sitting in a filing cabinet. And some confidential information still is! InfoSec is concerned with making sure data in any form is kept secure and is a bit broader than cybersecurity. So, someone could likely be an information security expert without being a cybersecurity expert.

“Yes” or “no” questions won’t help you better understand your vendors’ (or your) cybersecurity posture—but actionable metrics will.

CYBERSECURITY
Cybersecurity is all about protecting data that is found in electronic form. Part of that is identifying what the critical data is, where it resides, and the technology you have to implement in order to protect it.

OVERLAP BETWEEN INFORMATION SECURITY & CYBERSECURITY

There is a physical security component to both cybersecurity and information security.

If you have a warehouse full of confidential paper documents, you clearly need some physical security in place to prevent anyone from rummaging through the information. And as more data becomes digital, the process to protect that data requires more advanced IT security tools. So, while you can’t put a physical padlock on a desktop computer, you can put a padlock on your server room door. In other words, if your data is stored physically or digitally, you need to be sure you have all the right physical access controls in place to prevent unauthorized individuals from gaining access.

They both take the value of the data into consideration.

If you’re in information security, your main concern is protecting your company's data from unauthorized access of any sort—and if you’re in cybersecurity, your main concern is protecting your company’s data from unauthorized electronic access. But in both scenarios, the value of the data is of utmost importance. Both individuals need to know what data is most critical to the organization so they can focus on placing the right controls on that data. In some scenarios, an information security professional would help a cybersecurity professional prioritize data protection—and then the cybersecurity professional would determine the best course of action for the data protection. But with the changing security landscape over the past decade, things aren’t always this black and white.

THE EVOLUTION OF INFORMATION SECURITY & CYBERSECURITY
Over the last decade, we’ve seen a fusion between cybersecurity and information security, as these previously siloed positions have come together. The challenge is, most teams don’t have an information security professional on staff—so the responsibilities of a cybersecurity professional have expanded dramatically. Cybersecurity professionals traditionally understand the technology, firewalls, and intrusion protection systems needed, but weren’t necessarily brought up in the data evaluation business.

But today, that is changing. As this subject becomes increasingly important for businesses, the role of cybersecurity experts is evolving so they can properly protect data. Business partners and investors are increasingly aware of the importance of this topic, and companies are asked regularly about their effectiveness in securing data and managing risk in both cyber and physical forms.

IN SUMMARY
Because of the evolution of this position, it’s easy to understand why many people discuss cybersecurity and information security in the same breath. And, you can see how the questions that information security and cybersecurity try to answer are, in essence, the same:
1. How do we define what data is critical to us?
2. How do we protect that data?

This article is from BITSIGHT, https://www.bitsighttech.com/blog/cybersecurity-vs-information-security

Hackers are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say
By NICOLE PERLROTH, the New York Times, July 7, 1017


Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries.

Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week.

The joint report was released on June 28. It was obtained by The New York Times and confirmed by security specialists who have been responding to the attacks. It carried an urgent amber warning, the second-highest rating for the severity of the threat. The report did not indicate whether the cyberattacks were an attempt at espionage — such as stealing industrial secrets — or part of a plan to cause destruction. There is no indication that hackers were able to jump from their victims’ computers into the control systems of the facilities, nor is it clear how many facilities were breached.

Wolf Creek officials said that while they could not comment on cyberattacks or security issues, no “operations systems” had been affected and that their corporate network and the internet were separate from the network that runs the plant.

The hackers appeared determined to map out computer networks for future attacks, the report concluded. But investigators have not been able to analyze the malicious “payload” of the hackers’ code, which would offer more detail into what they were after.

John Keeley, a spokesman for the Nuclear Energy Institute, which works with all 99 electric utilities that operate nuclear plants in the United States, said nuclear facilities are required to report cyberattacks that relate to their “safety, security and operations.” None have reported that the security of their operations was affected by the latest attacks, Mr. Keeley said. In most cases, the attacks targeted people — industrial control engineers who have direct access to systems that, if
damaged, could lead to an explosion, fire or a spill of dangerous material, according to two people familiar with the attacks who could not be named because of confidentiality agreements.

The origins of the hackers are not known. But the report indicated that an “advanced persistent threat” actor was responsible, which is the language security specialists often use to describe hackers backed by governments. The two people familiar with the investigation say that, while it is still in its early stages, the hackers’ techniques mimicked those of the organization known to cybersecurity specialists as “Energetic Bear,” the Russian hacking group that researchers have tied to attacks on the energy sector since at least 2012. Hackers wrote highly targeted emails messages containing fake résumés for control engineering jobs and sent them to the senior industrial control engineers who maintain broad access to critical industrial control systems, the government report said.

The fake résumés were Microsoft Word documents that were laced with malicious code. Once the recipients clicked on those documents, attackers could steal their credentials and proceed to other machines on a network. In some cases, the hackers also compromised legitimate websites that they knew their victims frequented — something security specialists call a watering hole attack. And in others, they deployed what are known as man in the middle attacks in which they redirected their victims’ internet traffic through their own machines.

Energy, nuclear and critical manufacturing organizations have frequently been targets for sophisticated cyberattacks. The Department of Homeland Security has called cyberattacks on critical infrastructure “one of the most serious national security challenges we must confront.”

On May 11, during the attacks, President Trump signed an executive order to strengthen the cybersecurity defenses of federal networks and critical infrastructure. The order required government agencies to work with public companies to mitigate risks and help defend critical infrastructure organizations “at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.” The order specifically addressed the threats from “electricity disruptions and prolonged power outages resulting from cybersecurity incidents.”

Jon Wellinghoff, the former chairman of the Federal Energy Regulatory Commission, said in an interview last week that while the security of United States’ critical infrastructure systems had improved in recent years, they were still vulnerable to advanced hacking attacks, particularly those that use tools stolen from the National Security Agency.

“We never anticipated that our critical infrastructure control systems would be facing advanced levels of malware,” Mr. Wellinghoff said.

In 2008, an attack called Stuxnet that was designed by the United States and Israel to hit Iran’s main nuclear enrichment facility, demonstrated how computer attacks could disrupt and destroy physical infrastructure. The government hackers infiltrated the systems that controlled Iran’s nuclear centrifuges and spun them wildly out of control, or stopped them from spinning entirely, destroying a fifth of Iran’s centrifuges. In retrospect, Mr. Wellinghoff said that attack should have foreshadowed the threats the United States would face on its own infrastructure.

Critical infrastructure is increasingly controlled by Scada, or supervisory control and data acquisition systems. They are used by manufacturers, nuclear plant operators and pipeline operators to monitor variables like pressure and flow rates through pipelines. The software also allows operators to monitor and diagnose unexpected problems. But like any software, Scada systems are susceptible to hacking and computer viruses. And for years, security specialists have warned that hackers could use remote access to these systems to cause physical destruction.

---

Copycat malware infects 14M Android devices, steals credits for app downloads

Bradley Barth, SC Media, Jul 06, 2017

A mobile malware that roots Android devices and commits both ad and app fraud has infected at least 14 million devices, at one point raking in $1.5 million during a peak two-month period in 2016, Check Point Software Technologies has reported.

Dubbed Copycat, the malware is the first known adware that injects its code into Zygote, a daemon tasked with launching apps on Android devices. This dangerous technique gives the malware an extremely strong foothold on affected devices, allowing it to infiltrate the activity of all running apps, Check Point explained in a blog post and accompanying technical report.

Significantly, Copycat steals credits earned by legitimate advertisers whenever one of their ads results in an application download. The malware accomplishes this by swapping out the ad company's real referrer ID with a fraudulent one. These credits are ultimately exchanged for revenue. According to Check Point researcher Daniel Padon, this technique has never been seen before, and is more lucrative than traditional ad fraud.

"There are many efforts by ad networks to detect and stop fraud from happening and this is actually a... way to do it without being detected," said Padon, in an interview with SC Media. "You have to be on the device itself [and monitoring] device activity to understand that fraud has actually taken place." Otherwise, the ad transaction "will look like a legitimate one from end to end."

Copycat specifically scams Tune, a mobile analytics platform that tracks advertisements that result in a viewer downloading an app. According to Check Point's blog post, when an infected user visits Google Play, "Copycat retrieves the package name of the app that the user is viewing on Google Play, and sends it to its command and control server. The server sends back a referrer ID suited for the package name. This referrer ID belongs to the creators of the malware, and will later be used to make sure the revenue for the installation is credited to them. Copycat blocks all install referrer intents and replaces them with its own referrer ID, which was received from the command and control server previously."

Victims of Copycat were infected by downloading malicious apps distributed by third-party stores unaffiliated with Google Play. Upon reporting Copycat to Google in March 2017, Check Point learned from Google that the company had been aware of the campaign and had already taken steps to curtail its damage. Consequently, there are now fewer current infected devices than there were during Copycat's two month peak period from April to May 2016, when it generated the vast majority of its revenue. (The earliest evidence of Copycat traces back to March 2016, said Padon.)

"Copycat is a variant of a broader malware family that we've been tracking since 2015," a Google spokesperson told SC Media in an emailed statement. "Each time a new variant appears, we update our detection systems to protect our users. Play Protect secures users from the family, and any apps that may have been infected with Copycat were not distributed via Play. As always, we appreciate researchers' efforts to help keep users safe."

The 14 million devices found infected by Copycat are all linked to one command and control server, meaning there could be additional C&Cs linked to millions more victims. Of this lot, 55 percent of devices are based in Asia, with a heavy concentration in the Southeast Asia region, including India (3.84 million infections), Pakistan (1.06 million), Bangladesh (1.03) and Indonesia (1.01 million). Africa saw 18 percent of infections and the Americas experienced 12 percent, with 280,000 infections in the U.S.

Eight million of the infected devices, or about 54 percent, were successfully rooted, a usually high share, Check Point noted.

In addition to stealing credits for app downloads, Copycat also makes money by fraudulently delivering ads and downloading apps. Of the 14 million phones infected with the malware, 4.9 million were made to serve up apps, 4.4 million stole credits for app downloads and 3.8 million issued ads to their owners, Check Point reported. The app fraud activity generated $735,000 in ill-gotten revenues, while the credit stealing activity yielded at least $660,000 by very conservative estimates. The ad fraud activity has been responsible for displaying around 100 million ads, collectively worth around $120,000.
Regarding attribution, Check Point said that its researchers found some notable links between Copycat and MobiSummer, an ad network based in China. For instance, the malware contains code signed by MobiSummer and uses remote services created by the ad network. Also, the two entities share a common server. While previous adware campaigns have been linked to Chinese online ad companies, it is also possible that CopyCat's authors could have simply borrowed MobiSummer's various assets without permission.

**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.

Where: Looking for a New Location
When: New Location means new days… looking at 2 times per month

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

Director of Education, Larry Dilley
certification@kc.issa.org
ISSA International Conference, October 9-11 in San Diego!

- **Registration is open!** Please use the attached Event Marketing Toolkit to share information about the conference to your members and share on social media using hashtag #ISSAConf. I have also includes some slides you can add to your deck to share information about the conference during an upcoming chapter meeting.
- We are also seeking conference volunteers to help with some on site tasks and in exchange, offer a discounted or complimentary conference pass. For more information, visit our [On Site Volunteer Schedule and Sign-up Sheet](#). Please feel free to share with your members!

### 2017 CIO Agenda: A Security and Risk Management Perspective

*Gartner: Join us for 60 minutes: 2pm AEST | 12midnight EDT | 4am GMT*

**Discussion Topics:**
- What the main elements are for the 2017 CIO Agenda
- What the implications are for security and risk management leaders

Hosted by: Rob McMillan, Research Director

The 2017 CIO Agenda highlights the importance of building a digital ecosystem for enterprises. Security and Risk Management leaders must understand CIO priorities and incorporate Security and Risk Management practices into the digital ecosystem to reap growth benefits.

**ATTEND**
Top Cybersecurity Trends for 2017-2018

**Gartner: Join us for 60 minutes**

Discussion Topics:
- What technology and market trends are occurring to meet the changing digital security landscape?
- Which security technologies & processes have changed to accommodate the demands of digital business?
- How digital security leaders in organizations can use these trends to their advantage

Hosted by: Earl Perkins, Research VP

Security concerns continue as organizations globally grapple with technology changes affecting them. Threats to that technology and supporting process continue to grow in number and sophistication. Traditional IT security leaders have become digital security leaders as they expand support to address risks for technology-savvy engineering and physical environments while embracing expanded roles for cloud and mobile services. This webinar reviews the lessons learned and informs listeners how to use the past to create the future.

**ATTEND**

**ISSA 2017 Fellows Cycle**

2017 Fellows Cycle is Now Open

The Fellow Program recognizes sustained membership and contributions to the profession. 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. The next cycle will open December 2, 2016 and applications will be accepted until July 10, 2017 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 for the 2017 Cycle will be recognized at the 2017 ISSA International Conference. Submissions received after the deadline will not be considered.

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

**Become a Senior Member**
- Any member can achieve Senior Member status, the first step in the Fellow Program. What are the criteria?
- 5 years of ISSA membership
- 10 years relevant professional experience
- All Senior Member applications require an endorsement from their home chapter to qualify
- For your convenience, please feel free to use this Senior Member Application Check-list to confirm eligibility and completion of application

**Application forms:**
- Submit your application for Senior Member
- Submit an endorsement on behalf of a Senior Member candidate
Fellow and 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 consult the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

Fellow Qualifications
- 8 years of association membership
- 12 person-years of relevant professional experience
- 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
- All Fellow applications require a nomination to qualify
- For your convenience, please feel free to use this Fellow Application Check-list to confirm eligibility and completion of application

Application forms:
- Submit your application for Fellow
- Submit a nomination on behalf of a Fellow candidate
- Submit a letter of recommendation on behalf of a Fellow candidate

Distinguished Fellow Qualifications
- 12 years association membership
- 16 person-years of relevant professional experience
- 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
- For your convenience, please feel free to use this Distinguished Fellow Application Check-list to confirm eligibility and completion of application

Application forms:
- Submit your application for Distinguished Fellow
- Submit a nomination on behalf of a Distinguished Fellow candidate
- Submit a letter of recommendation on behalf of a Distinguished Fellow candidate

Please send an email if you have any questions about the ISSA membership and benefits.

Thanks,
Membership Director, membership@kc.issa.org
July 27, 2017 ISSA Chapter Meeting

Speaker: Bryan Bailey
Bio: Cyber security sales executive with extensive experience in network security, demand generation, partnering with the customer at all levels, learning new technology, top down selling and closing business in complex selling environments.

Specialties: utilities, telecom service providers, wireless (3G / 4G LTE, WiMax, Small Cells, 802.11, Micro Networks) broadband, networking, cold calling, direct marketing, sales strategy, IP, multimedia, networks, outside sales, finding the decision maker, program management, sales development, teaching, negotiation, and Ethernet.

Topic: Bypassing your network security – how likely is it?
How likely is a breach to your network security? What’s the global view of network security today? Show the latest NSS Labs report on which vendors are doing the best with Zero Day threats and Malware. Evasions defined! What is Evador?

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

Menu:
Salad
Choice of Chicken, Salmon and 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