Hello ISSA Kansas City Members. Hope all of you had a wonderful holiday and Happy 2016!

In kicking off 2016, I would like say we had a memorable 2015! I would like to express a great deal of gratitude to ISSA KC board members for their time and significant contributions to this organization.

My focus will be on achieving the following in 2016 similar to last year. Overarching goal is to ensure our ISSA Kansas City members have a meaningful experience in 2016.

Objectives:
1. Ensure we have quality content presented month over month
2. Ensure we meet at suitable and desirable venues and networking events
3. Ensure our member majority interests are incorporated into our program planning continuously
4. Ensure our members receive timely communication updates.

Thank you for participating in the elections for ISSA KC board officers! We will be announcing the results next month. If you are interested in any roles and did not participate in the voting survey, please let me know.

Sincerely,

Naeem Babri
President, ISSA Kansas City

Upcoming ISSA-KC Monthly Chapter Meeting Schedule

**January 28, 2016**
**ISSA Chapter Meeting**
**Radware**
Hereford House

**February 25, 2016**
**ISSA Chapter Meeting**
**OpenDNS/CISCO**
Lidia’s Italy of KC

**March 24, 2016**
**ISSA Chapter Meeting**
**Dell**
Rye’s (Tentative)
On December 10, 2015 the ISSA-KC Chapter members, ISACA, and other security professionals held a meeting at Ritz Charles of Overland Park to network and attend the monthly chapter meeting, with presentation topic. The topic of discussion was the Verizon DBIR: Beyond the Hype Incident Report. The Verizon Data Breach Incident Report is one of the most read reports in InfoSec, but most people don't really dig into the report and its underlying wealth of information. In this presentation, Jack Daniel of Tenable Network Security and Gabriel Bassett of Verizon focused on three keys areas: (1) Analysis beyond the bullet points in the DBIR, and follow-up analysis beyond the initial report, (2) The value of the Vocabulary for Event Recording and Incident Sharing (VERIS) framework for describing security incidents in a structured and repeatable manner and (3) Making the DBIR Actionable: how to apply the lessons and data from the DBIR and other reports to make your environment more secure. Approximately 70 members from ISSA and ISACA attended the meeting.

ISSA and ISACA Combined Meeting Recap
Authentication proves who we are. Access controls allow us to gain access to systems and information. There are several popular access control models such as discretionary access control (DAC), mandatory access controls (MAC) and role based access controls (RBAC). There has been much discussion on where and how to implement different access models, should it be done in a centralized manner or decentralized. Discussed here are the three models presented, with commentary on a recommended model to be used, along with if access control should be centralized or decentralized?

The Role-based Access Control (RBAC) model also called the non-discretionary access control model uses a centrally administered set of controls to determine who subjects and objects interact (Harris, 2010). This type of model grants access based on the employees role and what they do for the company. Using this model the owner of the asset determines what privileges to assign to the employee and the security administrator adds the privileges to the user ID and groups that are created by the administrator. Roles and groups act as containers. This type of model is ideal for companies who have a high turnover rate. In summary these type of model the access decisions are based on the subject’s role.

Discretionary Access Control (DAC) is when the data owners decide who has access to what resources. The model is called discretionary because the control of access is based on the discretion of the owner. Discretionary Access Control allows the user to control access to their own data. This model is the least restrictive because a subject has total control over any objects that he or she owns. A subject can also change the permissions for other subjects over objects (Harris, 2010). Desktops operating systems generally use the default access control DAC model.

Mandatory Access Control (MAC) model in contrast to the DAC model has the most security, and is the most restrictive, because all controls are fixed. MAC has security labels assigned to all resource objects on the system. These security labels contain a classification such as top secret, confidential secret. Security labels are attached to all objects and all users must have a secret clearance. This framework is based on security clearances (top secret, secret, etc.) which we often find in the government sector, department of defense, and the military. In reference to centralized versus centralized authentication systems the author of this article prefers centralized authentication, or what is commonly referred to today as Single Sign-On (SSO) technology. In today’s information systems environment companies strive to ensure that users only have to authenticate once, but are able to access any network resources that they have a need to do their job. The single sign-on technology allows companies to design the infrastructure which will allow remote access to technologies; rather it is via a VPN or access to email, web services, and files. The MAC model is used in the military where confidentiality is important. For example a user with top secret classification cannot access a resource if they are not also a member of one of the required categories for that object. Also a user with a secret clearance cannot access an object with a top secret security label.

Depending on the environment any number of these access control frameworks will work for software developers who need to implement access control in their devices or applications. However, I think the Role-Based Access Control Model provides a more real-world approach. A centralized framework for authentication is ideal; centralized authentication approach requires hosts to trust and follow the policies defined by a central authentication authority and the ability to maintain the systems are more flexible and cost effective. Additionally, with centralized authentication ideally all users will have one account for authentication to
multiple systems/hosts, which helps with user account management. Although, I will agree that a true centralized authentication is rarely achievable and hybrids are used in most large to medium size companies.

Reference

Author,
Cheryl O. Cooper, CISSP and ISSA KC Chief Editor

---

**Certification Corner**

The Official (ISC) 2 Guide to the CISSP CBK, 7th Edition is now available. This edition reflects the changes to the CBK that are effective April 15th, 2015. The digital download is available via the official (ISC) 2 website at [https://www.isc2.orgofficial-isc2-textbooks.aspx](https://www.isc2.orgofficial-isc2-textbooks.aspx). These books can also be purchased through Amazon.

Thanks,
Director of Education
certification@kc.issa.org

---

**ISSA Kansas City Chapter New Members and Membership Renewals**

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

Thanks,
Membership Director, membership@kc.issa.org

---

**Save the Date — February, 2016**

**ISSA February Chapter Meeting**
**Speaker:** Open DNS  
**Duration:** 1 hour  
**Location:** Lidia’s Italy of Kansas City

---

**Events, Training and CPE Opportunity**

**ISSA January 2016 Journal**

Members - Please click on the following Journal issue links for access:  
[Bluetoad](#) | [PDF](#) | Mobile: [ePub](#) | [Mobi](#)

**Webinars & Conferences**

Webinars are an easy way to stay informed on trending industry developments from the convenience of your own office. In everything from [mobile technology](#) to [compliance](#). Webinars and conferences provide insight into topics affecting our industry and your business.

**WEBINAR: EU Data Protection Regulation: New Legal Considerations for Security Professionals**

**Date/Time:** 28 Jan 2016, 15:00 GMT, 10:00 EST
How the upcoming EU data protection regulation is forcing businesses to change. The upcoming EU General Data Protection Regulation means all businesses risk massive fines and potential compensation sanctions should they fail to protect customer and employee personal identifiable information. Law firms are assessing requirements and the pressure will be on your organization to be prepared. In this Webinar, you will learn more about:

- The present state of the EU General Data Protection Regulation
- The upcoming changes and what they mean to you
- What you can do to best prepare for the new legislation

Join this webinar and learn how to protect yourself, your data and your business. Register

Tim Hoffman & Associates values and prioritizes the learning of each ISSA member. As part of their mission, they support the CISSP certification by offering an 8 week CISSP ONLINE TRAINING course. This is the easiest and most cost-effective way to acquire the certification.

Tim Hoffman & Associates is dedicated to supporting ISSA members in their professional growth. They offer an 8-week online study course for $189.
This price includes:
- A hard copy of The Official Guide to CISSP CBK by Adam Gordon
- Slides that outline the material in the book.
- Weekly summaries and daily quiz questions.
- Online study reference materials.

Click the link below to register:
http://www.timhoffmanassociates.com/classes/
Check our website:
http://www.timhoffmanassociates.com

January, 2016 Chapter Meeting

ISSA-Kansas City January, 2016 Chapter Event

On January 28, 2016 the ISSA-KC Chapter members and other security professionals will hold a meeting at Hereford House to network and attend the monthly chapter meeting, with presentation topic.

Speaker: Carl Herberger

Topic: "Safety, Sanctuary and Security: The Societal Impact of Ever-Permeating Connectivity"

Summary: Every day, we network-enable more aspects of our professional and personal lives. We make conscious decisions to adopt technologies in the pursuit of convenience or an apparent need to feel connected. Often the decisions are thrust upon us by employers, service providers or even those we’ve come to rely on in the physical world. Each step towards deeper and total connectivity comes with consequences; risks associated with our personal privacy, the security of our business and even our safety. In this session, Radware will explore the changes we’ve already allowed into our lives, where things are leading, and portents for personal, business and public security.

Bio: Carl Herberger is the Vice President of Security Solutions at Radware, a leader in application delivery and security solutions that assures the availability, performance, and resilience of business-critical applications for over 10,000 enterprises and carriers worldwide. Carl, a recognized information security expert, draws on his extensive information security background in both the private and public sectors. He began his career in the U.S. Air Force as a computer warfare specialist at the Pentagon and managed critical operational intelligence programs aiding both the National...

**Location:**
Hereford House 5001 Town Center Drive, (Near W 117th St and Roe Ave)
Leawood, KS 66211
(913-327-0800)
http://www.herefordhouse.com/leawood.php

**Agenda:**
12:00 PM - 1:00 PM - Meeting & Presentation
1:00 PM - 1:30 PM - Questions, Answers & Networking

**Lunch Menu:** Choice of Beef, Chicken, or Salmon includes Salad, Potato, Vegetable, and Drink

Vegetarian option available, please inquire upon registration for the event.

**Price:**
Members: $20.00
Non-Members: $30.00

**Maximum Reservation:** 40
Credit(s): 1 CPE credit

To Register, please use one of the following links:

*** 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/Program Director
Dan Boeth
vp@kc.issa.org

Director of Social Media
Melissa Salazar

Secretary of Board
Cheryl Cooper

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

Treasurer
treasurer@kc.issa.org

Director of Membership
membership@kc.issa.org

Director of Education
certification@kc.issa.org

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

Webmaster
Thomas Badgett
webmaster@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood