



The President's Corner

Upcoming Events

Inside This Issue

- Presidents Corner
- Chapter News
- Webinar/Conferences
- Upcoming Event
- Membership Corner
- Certification Corner
- Security & Privacy
- Sponsors

Happy July!

Hope you enjoyed last month's presentation on MITRE ATT&CK. If you are interested in serving on the ISSA KC board as a member or committee member, please reach out to me at president@kc.issa.org.

Information Systems Security Association Int is pleased to announce the dates and location of this year's ISSA International Summit! Join us in Irving/Dallas, Texas - October 1-2, 2019!

Did you know, ISSA Internal Board President is Candy Alexander, VP is Roy Wilkinson, Secretary is Anne M Rogers and Treasurer is Pamela Fusco. Board of Directors are Mary Ann Davidson, Ken Dunham, Alex Grohmann, Shawn Murray, Deborah Peinert, Wayne Proctor, David Vaughn, and Stefano Zanero.

Sincerely,
Naeem Babri
President, ISSA-Greater Kansas City Chapter

Chapter Meeting
July 25th
12 Ways to Hack 2FA

Chapter Meeting
Sept 26th
More to come

Connect With Us
kc.issa.org

Twitter
KansasCityISSA

Facebook @kcissa

LinkedIn



Chapter News

ISSA Journal : July 2019

Feature articles include:

- Drone Hacking: Mirai in the Sky?
- Robotic Process Automation Meets Identity and Access Management
- OWASP: Application Security's Best Friend
- Security Standards Participation
- The Python Programming Language: GUI #2

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

Not a member? Read this month's feature article - [The Future of IT Risk Management Will Be Quantified](#) - at no charge or [Join Now](#) and gain full access to the *ISSA Journal*.

Webinars & Conferences



[INTERFACE-Kansas City](#)

Jul 18th, 2019

8:30 am – 4:30pm

Overland Park Convention Center
Ballrooms A-C
6000 College Boulevard
Overland Park, KS 66211

Register

<https://f2fevents.com/evite/kcm19-issa-kansas-city/>



[Register Now for Black Hat USA and Save!](#)

Black Hat USA will take place August 3-8, 2019 at the Mandalay Bay Convention Center. Black Hat USA Briefings will present the latest security research, Wednesday, August 7 and Thursday, August 8. View all announced Briefings abstracts and save \$200 when you register for your Briefings pass with code 19issa1

ISSA International Summit

Join cyber security professionals from around the world on October 1 - 2, 2019, in Irving, Texas, for the 9th annual ISSA International Summit

[LEARN MORE](#)

Please Support our Chapters and Partners!



**Join us Oct 1-2, 2019
in Irving/Dallas, TX for the
2019 ISSA International Summit**



Upcoming Chapter Event

July 25th Chapter Meeting:

Topic: 12 Ways to Hack 2FA

Topic Summary:

Everyone knows that multi-factor authentication (MFA) is more secure than a simple login name and password, but too many people think that MFA is a perfect, unhackable solution. It isn't! I can send you a regular phish email and completely take control of your account even if you use a super-doooper MFA token or smartphone app. Attend this webinar and learn the 12+ ways hackers can and do get around your favorite MFA solution. The webinar will include a (pre-filmed) hacking demo by KnowBe4's Chief Hacking Officer, Kevin Mitnick, and real-life successful examples of every attack type. It will end by telling you how to better defend your MFA solution so that you get maximum benefit and security.

Speaker Bio

Roger A. Grimes, Data-Driven Defense Evangelist for KnowBe4, Inc., is a 30-year computer security consultant, instructor, holder of dozens of computer certifications, and author of 10 books and over 1,000 magazine articles on computer security. He has spoken at many of the world's biggest computer security conferences, been in *Newsweek*™ magazine, appeared on television, been interviewed for NPR's *All Things Considered*™, and been a guest on dozens of radio shows and podcasts. He has worked at some of the world's largest computer security companies, including Foundstone, McAfee, and Microsoft. He has consulted for hundreds of companies, from the largest to the smallest, around the world. He specializes in host and network security, identity management, anti-malware, hackers, honeypots, Public Key Infrastructure, cloud security, cryptography, policy, and technical writing. His certifications have included CPA, CISSP, CISA, CISM, CEH, MSCE: Security, Security+, and yada-yada others, and he has been an instructor for many of them. His writings and presentations are often known for their real-world, contrarian views. He has been the weekly security columnist for *InfoWorld* and *CSO* magazines since 2005.

Location:

Lidia's Restaurant
101 W 22nd St, Kansas City, MO 64108

Agenda:

11:30AM - 12:00PM - Registration and Check In
12:00 PM - 1:00 PM - Lunch /Speaker's Presentation

Price:

\$25 members | \$30 guests

*** [Register](#) ***



Aug 22nd next Meeting!

Topic: Coming Soon!

Location: Brio

502 Nichols Rd, Kansas City, MO 64112

Agenda:

11:30AM - 12:00PM - Registration and Check In

12:00 PM - 1:00 PM - Lunch /Speaker's Presentation

Price:

\$25 members| \$30 guests

Membership

Please contact membership@kc.issa.org for question or concern when applying to be an ISSA Senior Member or ISSA Fellow

Senior Member, Fellow, and Distinguished Fellow applications are available. Please read and apply here:

<https://www.issa.org/page/FellowProgram>

Best Regards,
Director of Membership
Wei Cheng

Security & Privacy: Articles and News

Feature Articles

New York Legislature passes bill that toughens breach notification standards

By Bradley Barth

The New York State Legislature last month passed The Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which is intended to strengthen the state's data security laws by more explicitly defining when and how businesses must notify the public and attorney general of a data breach incident.

The proposed legislation, introduced by State Senator Kevin Thomas (D) and Assemblymember Michael DenDekker (D), now sits on the desk of Governor Andrew Cuomo, awaiting his signature.

Under current law, businesses must disclose a breach only when it is reasonably believed that an unauthorized person acquires certain personal and private information. But SHIELD would lower the threshold so that the reasonable belief that someone merely accessed the information is enough to require a notification.

[*** Continued](#)

Insulin Pumps Recalled By FDA For Cybersecurity Risks

By Phee Waterfield

The U.S. Food and Drug Administration (FDA) is warning patients and healthcare providers that some insulin pumps carry cybersecurity risks.

In an alert published on June 27 2019, the FDA said that certain Medtronic MiniMed™ insulin pumps carry potential cybersecurity risks and that patients with diabetes using these models should switch their insulin pump to other models.

The alert says: "The FDA has become aware that an unauthorized person (someone other than a patient, patient caregiver, or health care provider) could potentially connect wirelessly to a nearby MiniMed insulin pump with cybersecurity vulnerabilities." The alert goes on to say that a person could change a pump's settings to either "over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or stop insulin delivery, leading to high blood sugar and diabetic ketoacidosis." Both are life-threatening.

[*** Continued](#)

Mentor Program: ISSA Greater Kansas City

The program is designed to formalize relationships between senior professional individuals in the chapter (Mentors) and the various levels of security professionals seeking entry or moving through the different phases of this profession (Mentees). There are many different types of mentoring partnerships; peer to peer, adult to adolescent, apprentice to master, cross generational, and mentoring within a company or a few. It depends on what type of mentoring relationship you're seeking.

Mentor/Mentee application: [Mentor Application](#) :: [Mentee Application](#)

Feature Articles - continued

Continued News from Article Page

Premera Reaches \$10M Settlement with 30 States Over 2014 Data Breach

by Jessica Davis

After reaching a \$74 million settlement with the 10.4 million patients impacted by its 10-month hack, Premera Blue Cross signed an agreement with 30 states requiring the insurer to bolster its cybersecurity program.

July 12, 2019 - One month after settling with its data breach victims, Premera Blue Cross signed a \$10 million settlement with 30 states after a 10-month hack on its system breached the data of 10.4 million patients.

Washington Attorney General Bob Ferguson led an investigation into the breach, which was discovered by Premera officials in January 2015. However, the hack began in May 2014 and went undetected for 10 months.

Ferguson's team found that Premera failed to meet HIPAA obligations and violated state consumer laws, including the Washington State Consumer Protection Act, when it did not address known cybersecurity vulnerabilities.

According to Ferguson, Premera ignored repeat warnings from cybersecurity leaders and its own auditors about its inadequate security: "the company accepted many of the risks without fixing its practices."

The insurer misled consumers about its privacy practices before and after the data breach was detected and announced, when officials told the public "there were already significant security measures in place to protect your information," Ferguson said.

[*** Continued](#)

Sponsors

Board of Directors

Our Sponsors

President

Naeem Babri

Secretary of Board

Rochelle Boyd

Treasurer

Gary Kretzer

Director of Membership

Wai Cheng

Director of Education

Nicole Windholz

Director of Programs

Chris Mcleod

Webmaster

Thomas Badgett

CISSP Study Group

Mark Waugh

issakc-study@kc.issa.org

Past Presidents

Bob Reese

Tom Stripling

Jeff Blackwood

Michelle Moloney

