Information Systems Security Association
The Global Voice of Information Security

Kansas City ISSA Newsletter

May 24, 2018

Topic: Key Changes in Security and Why They Matter, AKA Data Swamps and Data Lakes

Securonix

Lidia's Italy

Inside this issue:

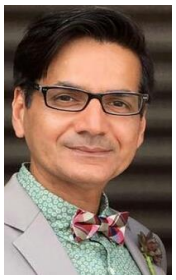
Volume 56, Issue 1 May 2018

The President's Corner

Hello ISSA Kansas City Members and Happy Spring!

Wishing you all happy May! Hope you enjoyed the April presentation on "Hot Topics in Information Security Law, from GDPR to Data Breach Class Actions" by Tedrick Housh. This month's topic is "Key Changes in Security and Why They Matter, AKA Data Swamps and Data Lakes", looking forward to seeing you all there at the May chapter meeting. We will have a great discussion.

ISSA has a CISO Executive Membership Program to give executives an environment to achieve mutual success. Connecting professionals to a large network of peers, valuable information, and top industry experts. The program is a functional resource for members to advance personal and industry understanding of critical issues in information security. Next ISSA CISO Executive Forum is in Denver, CO August 16-17, 2018. REGISTER NOW



Sincerely,

Naeem Babri

President, ISSA Kansas City

Upcoming ISSA-KC Monthly Chapter Meeting Schedule

May 24, 2018

Topic: Key Changes in Security and Why They Matter, AKA Data Swamps and Data Lakes

Securonix

Lidia's Italy

June 28, 2018

Topic: Enabling Business Transformation with a Strong Identity Foundation

Okta

BRIO's on the Plaza

July 26, 2018

Topic: More to Come

Hereford House, Leawood, KS.

ISSA KC April 2018 Meeting Recap

On March 26, 2018, the ISSA-KC Chapter members and other security professionals held a meeting at Hereford House restaurant to network and attend the monthly chapter meeting, on the topic: Hot Topics in Information Security Law, from GDPR to Data Breach Class Actions. Information Security professionals lead the battle to address vulnerabilities and avoid data loss or disclosure, but no system is perfect. Companies have to plan for what might go wrong, and the legal landscape, like security technology itself, changes quickly. Tedrick Housh of Lathrop Gage provided an update on the latest developments in the law of information security and data privacy, and answered a host of questions.

CONGRATULATIONS to the winner of the ISSA's $50.00 gift card give-away, John Goehrung!

From left to right naeem Babri, John Goehrung, Tedrick Housh

Security & Privacy Articles and News

Security Risk Assessments

Author: Dr. Cheryl Cooper, CISSP, Vice President ISSA

This article discusses security assessments and audits, with specific emphasizes on security assessments. An assessment is where you identify gaps and how to improve them. This paper discusses various ways you can do an assessment, including the best times, who should be involved, whether it should be done by internal or external people or by both. This paper primarily focuses on internal and external security assessments and common types of regulations that drive security and risk assessments.

Assessments

Security assessments are an evaluation to identify vulnerability deficiencies with the objective to develop mitigation plans to address weaknesses or gaps in a system or application compliance with a company's security policy. Although different from security audits, there are similarities. The goal of an assessment is to perform an evaluation on a system or information resources and provide a score on its measure of compliance with company policies and best practices.

Security assessments can be performed daily, weekly, or on monthly bases. These types of assessments are informal and generally are performed by internal personnel. Assessments can occur as a result of new technology or due to a software upgrade on an existing technology. Assessments are a snap shot in time and so therefore, should be performed routinely throughout the life cycle of the asset.

An organization should become proactive in managing security before the asset is placed in a production environment or when data has been created. According to Stallings & Brown (2012) information technology (IT) security management needs to be a key part of an organizations overall risk management plan (p. 469). The company should be proactive by creating a secure model to protect the asset in the planning stages, in doing so risk assessments are perform to meet this objective. For example, identifying firewalls, DMZ requirements, access controls encryption requirements, authentication, authorization, and auditing controls, as well as system hardening requirements could be a part of a security assessment (Stallings & Brown, 2012). An organization that purchases a technology to be installed in the enterprise should ensure that the device is in compliance with the company's policies by running security vulnerability scans to identify any non-compliance issues, such as lack of hardening of the operating system, missing patches, back door access, default passwords, and use of insecure protocols, i.e., Telnet, FTP, and "r" services.

How the identification of real and estimated threats contributes to security assessments

The identification of real and estimates threats contribute to the security assessment program of various technologies because it allows organizations to know what is at risks, as well as communicates to executives areas of non-compliance with laws and regulations. Organizations have a responsibility to implement authentication, authorization, and auditing controls to ensure the confidentiality, integrity, and availability of the data that is stored or transmitted. Measures that the IT team should take to maintain a high level of security is to implement a process to ensure that the applications remain in compliance by running periodic security scans to ensure systems are in compliance company policing, industry best practices, and regulatory standards as part of their internal security assessment program. Effective security management cannot exist in isolation. Security should be viewed as a companywide strategy to reduce overall security risks, as well as, to improve employee efficiencies and productivity across the business environment.

Foundation of a Security Management Program: Risk Assessments and Audits

Security assessments and audits are the foundation of any security company (Stallings & Brown, 2012). How can an organization ensure the confidentiality, integrity, and availability of resources and services if they are unaware of the security posture of their applications and threats to the organization? A security management program consists of risk assessments, security assessments, standards, guidelines, policies, and security awareness programs. The risk analysis identifies the company's assets, threats that put them at risks; estimated damage of the risks is exploited, as well as identifies the impact to the company (Stallings & Brown, 2012).

Compliance with Industry Standards and Regulations

Identification of threats to an enterprise contributes to compliance with industry standards and regulations, some of the most common are around patient healthcare information, customer personal network information, financial information, and protection of payment card information. Failure to adhere to these standards can result in excessive fines and penalties. The standards listed below drive internal and external security assessments:

- HIPAA: ensures protection of Personal Health Information (PHI) as stipulated by law to ensure the privacy of patient healthcare information. Failure to identify threats to the potential compromise of patient healthcare information can result in penalties (U.S. Department of Health & Human Services).
- Sarbanes-Oxley (SOX): companies must attest to its controls over financial information. Specifically this law provides standards around the auditing and the reporting of operational risks (Sarbanes Oxley Compliance, 2012). These laws were implemented as a result of company scandals such as with Enron and WorldCom.
- Payment Card Industry Standards: ensures companies acting as merchants must comply with the PCI industry standards to protect cardholder data. PCI standards provide a framework for companies to protect card holder data. If a company fails to identify threats to the exploitation of card holder data, they could face serious and stiff penalties (PCI Security Standards Council, 2012).
- Gramm-Leach-Bliley Act: this act ensures that companies provide customers privacy notices. Additionally, this acts ensures companies and financial institutions provide the option for customers to approve releasing and sharing their information with other third party entities (Harris, 2003, p 805).

- FCC Protection of Customer Proprietary Network Information (CPNI) - these laws require companies specifically telephone companies to protect customer call detail records and personal information. Companies must ensure they aware of the risks of compromising customer personal information because a violation of these laws it could result in fines or imprisonment (Federal Communications Commission).

Although this section only discussed a few of the laws and regulations, the point to be made is that identification of threats contributes to an application's security management because it ensures compliance with regulations.

Internal Security Assessments

Internal security assessments are performed by internal employees with some degree of experience about the technology, processes, and the organization. Internal security assessments are performed to identify if the controls in place are meeting the companies security policy and regulatory standards. Internal auditors generally work with the business units to identify gaps and security and work with the business unit to develop mitigation plans to bring the system, process, or technology in compliance. Internal assessments aid in preparation for independent third party audits and are critical for organizations that must be in compliant with regulatory and statutory laws such as HIPPA (Health Insurance Portability and Accountability Act), SOX (Sarbanes Oxley), PCI (Payment Card Industry) standards, and the GBLA (Gramm Leach Bliley Act). Employees within the organization identify if technology and processes are in conformance or non-conformance with regulatory, best practices and organizational security policies. A contrasting difference in internal and external assessments is internal assessments do not target people or groups of people whereas, external audits also monitor and target people.

External Security Assessments

External assessment in contrast to internal assessments is performed by an independent unbiased external organization or a consulting firm to assess and monitor the organizational procedures, and to measure if the organization complies with internal policies or standards set by the government. . External assessors provide an unbiased opinion versus providing a measurement of score that is provided when performing an internal assessment. Externally assessments can be more costly, especially for large size organizations in comparison to internal assessments in which the cost is built in the cost structure to operate the business. External assessments are ideal for organizations that must comply with regulatory and statutory laws such as HIPPA (Health Insurance Portability and Accountability Act), SOX (Sarbanes Oxley), PCI (Payment Card Industry) standards, and the GBLA (Gramm Leach Bliley Act).

Audits

According to Greene (2006) audits compare current practices against a set of standards and test to measure if systems are regulatory compliant. Some would say that there are three types of audits, security audits, security vulnerability assessments, and penetration testing. However, these are assessments that are one phase of a security audit. For example, penetration testing or what is commonly known as pen testing is to perform real-world attacks with the goal of identifying if the system can be compromised (Greene, 2006). This is one step in an all-encompassing audit that consists of multiple tasks and functions. One of the goals of an audit is to provide an opinion on the evidence, whereas with assessments they provide a score or a measurement of the system or applications' compliance with standards and best practices. Audits are generally performed by external third party professionals for financial institutions and other types of businesses, but can be performed by an internal auditor in preparation for an external audit.

The primary difference in an external security audit and security assessments is an audit measures the policies and procedures in an organization based on a set of established standards and is all encompassing and in-depth diagnosis of technology, processes, and people.

References
Federal Communication Commissions (n.d.). *Protecting customer proprietary network information (CPNI)*. Retrieved from, Federal Communication Commission's Web site: http://transition.fcc.gov/eb/CPNI/
Greene, S.S. (2006). *Security policies and procedures: Principles and practices*. Upper Saddle River, NJ: Pearson Education Inc.
Harris, S. (2003). *All-in-One CISSP certification exam guide* (2nd. ed.). Emeryville, CA: McGraw-Hill.
PCI Security Standards Council (2012). *PCI SSC data security standards overview*. Retrieved from, https://www.pcisecuritystandards.org/security_standards/index.php
Sarbanes Oxley Compliance (2012). *Sarbanes Oxley Act summary*. Retrieved from, Compliance Web site: http://www.sarbanes-oxley-compliance.us/
Stallings, W., & Brown, L. (2012). *Computer security principles and practice* (2nd ed.). Upper Saddle NJ: Pearson Education, Inc., publishing as Prentice Hall.
U.S. Department of Health & Human Services (n.d.). *The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security rule*s. Retrieved from U.S. Department of Health & Human Services, web site: http://www.hhs.gov/ocr/privacy/

SQL Injection

Author: Dr. Cheryl Cooper, CISSP, Vice President ISSA

Structured query language (SQL) injection is the number one threat to Web applications and associated databases. This brief article discusses SQL injection, and discusses how to counter this attack strategy.

SQL Injection

This section of the article discusses structured query language (SQL) injection in detail. SQL is an international standard that was developed by IBM (Stallings & Brown, 2012). It is a programming language that is used in relational database management systems (RDBMS) (Stallings & Brown, 2012). The main components of SQL within a database are; (1) the schemas, which describes the access controls and what users are available to view. The schemas also describe the structured of the database, (2) the tables which are columns and rows within the database that are located in tables, and (3) the views, which states who the access right to view the tables. The value of the views allows you to control what users can see. SQL allows you to query a database using commands such as, insert, select, update, or to locate data in a database (Stallings & Brown, 2012).

SQL Injection is a vulnerability that allows an attacker to retrieve information from a database. It is the most common application vulnerability, especially with web based applications. For example we know that credit card numbers, expiration dates, social security numbers and so on are stored in tables within a database. A SQL injection can occur when each time a user submits a query the application sends a command to the database to provide the information to the user (Gilad, 2008). This can be accomplished by either clicking on the mouse or by requesting the information from a keyboard. In this example an attacker could use the SQL Injection by inputting malicious code that manipulates the application to request illicit information or unauthorized information (Gilad, 2008). The whole goal of the attacker is to steal information. The most common place to gain access is via the client interface login screens on web pages because this is where a user enters their login credentials, usually a username and password as shown in figure 1 (Gilad, 2008). The html text will be look something like this to the following in figure 1 (Gilad, 2008):

Figure 1 Login Screen Example,

Username: Cheryl Cooper

Password: *******

Login

```
<html>
<body>
<table>
  <tr>
<td>Username:</td><td><input type="text" name="username" size="20"></td>
  </tr>
  <tr>
<td>Password:</td><td><input type="password" name="password" size="22"></td>
  </tr>
  <tr>
    <td colspan="2"><input type="submit" name="submit" value=Login/></td>
  </tr>
</table>
</body>
</html>
```

The attacker could then insert an SQL expression, be it a (“), (,) (&) (1=1), (1=true) or other characters and strings into the SQL language to execute arbitrary code, allowing him to gain access to all the user names and passwords in the database, to include the system administrator (Gilad, 2008). Another type of attack is to attempt to identify the structure of the database, by sending a HTTP request and SQL query the attacker could receive unauthorized information.

SQL Injection Defense Strategy

Some of the most common strategies are to use an application firewall, encryption, authentication, and ensure the system is designed for input validation (Gilad, 2008). Logging is another defense, and although it cannot prevent an attack it can be used as a detection control. Patch updates should be checked and performed on regular bases. Companies should implement processes to regularly run an application layer scans to identify vulnerabilities. Additionally, an input validation control should be implemented that validates the user before processing the request. Limiting permissions to prevent SQL injection attacks is another defense, limiting the permission to for example, read only, even if the attacker gained access he could only read versus delete or modify tables.

References

Gilad, R. (2008, July). *SQL injection*. Retrieved from, http://www.articlesdepot.info/Internet_&_Technology/Entry_6/SQL_Injection_for_Dummies.html

Stallings, W., & Brown, L. (2012). *Computer security principles and practice* (2nd ed.). Upper Saddle NJ: Pearson Education, Inc., publishing as Prentice Hall.

Attributing the Problem with Attribution in Cyberspace

Author: Elliott Lillard, ISSA Member

This article provides an opinion on the Attribution problem, especially concerning the conflict between the United States and foreign adversaries like China or Russia. Acting within cyberspace especially during hostile times and dealing with rival

nation states adds a lot of complexity in terms of determining risk and appropriate action. Attribution deals with the ability to thoroughly understand who is behind an attack. Attribution can be deciphered based on evidence provided from the action, previous facts of various actors at play in terms of victim and perpetrator, as well as the reward of understanding the who and why behind a cyber-attack.

Derek S. Reveron, the author of Cyberspace and National Security provides insights behind the problem of attribution, especially so in terms of cyberspace and cyberwar. "The increasing Internet accessibility of secrets, money, and industry creates significant incentives for individuals, groups, and states to find ways to use offensive cyber capabilities. This motivation is heightened by the fact that attributing attacks from cyberspace is often impossible and the laws and social norms relating to cyber espionage, crime, and warfare are often weak or nonexistent...As a result, those who profit from cyber-attacks are unlikely to be apprehended and if caught seldom face punishment," (Reveron, 91).

The underlying fact behind why various nation states, hacktivists, internal actors and rogue individuals pursue hostile acts that conducted anywhere else besides the cyberspace domain would be considered an act of aggression comes down to the fact that malicious actors feel that they can get away with the crime without any sort of negative consequence. It is also very difficult to understand the full extent of the damage behind a cyber-attack. "The opaque nature of actions in cyberspace makes it difficult for the defender to know how far the attacker has penetrated and, therefore, exactly where they are on the policy slope," (Hare, 132). Cyberwar is a far different battleground than traditional boots on the ground combat. It is much easier to understand who is behind missile strikes when the trajectory of artillery can be traced back to a hostile regime and thus be responded with equal or elevated kinetic action as well as to fully understand the damage done by such an attack.

At the time of this writing, the United States faces a few rival nations that could benefit from a successful and damaging cyber-attack. Those nation states include but are not limited to Russia, China, North Korea, and Iran. Russia has been under the microscope recently as it came to surface that they had direct impact on the last U.S. presidential election which threatens our democracy and outcome of a fair and just election process. China has gained economic benefits from conducting clandestine operations seeking intellectual property, trade secrets, and classified government documents. Iran and North Korea are increasingly interested in our nation secrets related to nuclear arms production and storage. These rival nations have made actions to infiltrate our nation and extract sensitive materials. However, these actions are not limited to passive actions and could be a more direct and crippling attack if focused on disrupting our critical infrastructure.

"A nation can suffer an existential threat from attacks and infiltrations through cyberspace by either state or organized non-state actors to degrade or disrupt critical infrastructure systems, both privately and publicly owned," (Hare, 127). The issue of attributing these hostile actions from these attacks back to the original actor is paramount to responding, mitigating and preventing future cyber-attacks.

Rival nation states will continue to ramp up their sophistication and frequency of these cyber-attacks to avoid detection. If not fearful of the consequence of their actions, there would be no reason to hesitate to issue further attacks against our democracy and way of life. "Deterring attacks has depended on convincing opponents that the costs of attacking would be greater than any benefits they might obtain," (Reveron, 92). The United States must ramp up the ability to catch cyber-attacks in action before damaging effects can be done and determine who is behind these attacks through attribution. Once an attack has been traced back to an actor there should be standards in place to understand and respond appropriately through direct action or forming a coalition of allies to freeze trade agreements, economic sanctions or bolster together to issue a reciprocating cyber-attack far worse than their original. "Inaction is easy to justify in a deterrence situation, as a would-be adversary can always claim other reasons for not conducting an action for which a victim threatens retaliation," (Hare, 131). By doing nothing after an attack also does nothing to deter future cyber-attacks.

Preventing future attacks is vital in successful deterrence strategy. "In most cases of cyber conflict confronting developed nations today, the more pressing issue is not deterring an actor from choosing to conduct hostile intrusions in cyberspace but compelling them to stop conducting intrusions that already have been highly successful," (Hare, 126).

Foreign adversaries such as Russia or China will continue to push boundaries, infiltrate our networks for secrets and potentially wreak havoc on our critical infrastructure and vital systems. Thus, emphasis will need to be made to not only

prevent future zero-day attacks but also prevent repetitive intrusion attacks that have already been proven to be successful. "Attribution is central to deterrence [...] [and] retaliation requires knowing with full certainty who the attackers are," (Hare, 128). Fixing the attribution problem in cyberspace will prevent future attacks because attackers will be caught in their tracks, responded to with appropriate action, and other nations will view this activity and think twice before conducting hostile actions.

Works Cited

Hare, F. (n.d.). The Signifi cance of Attribution to Cyberspace Coercion: A Political Perspective [Scholarly project]. Retrieved April 22, 2018, from https://ccdcoe.org/sites/default/files/multimedia/pdf/2_5_Hare_TheSignificanceOfAttribution.pdf

Reveron, D. S. (2012). Cyber challenges and national security: Threats, opportunities, and power in a virtual world. Washington, D.C.: Georgetown University Press.

2018 Global Threat Report

Presented by CrowdStrike

The 2018 CrowdStrike Global Threat Report offers one of the industry's most comprehensive reports on today's most damaging cyberattacks and dangerous adversaries. It contains valuable insights into the evolving threat landscape and includes recommendations that will help you be better prepared for the security challenges your organization faces now and in the future. Download this industry-leading report which explores many critical topics including:

- The distinctions between state-sponsored actors and cybercriminals and their different styles of crime;
- Why malware-based attacks continued to flourish over the past year, even when traditional antivirus products were present;
- Why government, healthcare and financial organizations continued to be highly targeted, but the hospitality industry emerged as a target of both e-Crime and nation-state actors.

READ NOW

https://www.databreachtoday.com/whitepapers/2018-global-threat-report-w-4181

ISSA Kansas City Chapter Mentor Program 2018!

The program is designed to formalize relationships between more 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). Since 2018 is the pilot year for this program for our chapter we need your participation to make it successful!

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.

CALL FOR MENTORS

BE A GAME CHANGER!

Complete and submit a Mentor/Mentee application:

Mentor Application

Mentee Application

Why should I be a mentor?

Contribute to the professional development of the future workforce;
Help build stronger community fabric;
Impart the principles of an experienced security professional;
Gain a broader view of your own community; and
Give something back to the profession!

ISSA Journal May 2018

May 2018

Volume 16 - Issue 5

Feature articles include:

- Practical and Actionable Cybersecurity Solutions for Securing Protected Health Information | Sue Wang and Zach Furness
- Orchestration and Automation in the Real World | Ken Dunham
- Security Threats, Defenses, and Recommended Practices for Enterprise Mobility | Vincent Sritapan and Karim Eldefrawy
- Securing a Medical Device | Dave Presuhn and Andrew Bomett
- Securing the Remote Employee: Protecting the Human Endpoint in the Cybersecurity Environment | Curtis Campbell

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 - Practical and Actionable Cybersecurity Solutions for Securing Protected Health Information - at no charge or Join Now and gain full access to the *ISSA Journal*.

Certification Corner

CISSP® Certified Information Systems Security Professional

ISC2 CISSP CERTIFICATION 2018 CHANGES

For those of you with the CISSP certification, or those who are pursuing a CISSP certification, there will be changes in 2018. Effective April 15, 2018, the CISSP exam will be based on a new exam outline, and the domains and their weights will change. The delivery method will change to Computer Adaptive Testing (CAT) that provides fewer questions in less time. There will be 100 to 150 questions, versus the 250 questions that were offered on the linear fixed exam that many of us have taken. The exam will no longer be up to 6 hours to complete, but up to 3 hours, on the average of 2 hours to complete. For more information on the changes, check out ISC2's web site, https://www.isc2.org/Certifications/CISSP

CALL for CISSP Instructors

ISSA is preparing their annual "CISSP Study Group Boot Camp" and we need instructors, preferably with a CISSP but not required. The boot camp study group is tentatively scheduled for September, 2018. If you are interested in being an instructor for one of the CISSP domains contact certification@kc.issa.org

Contact: Nichole, Director of Education/Certification, at certification@kc.issa.org

Contact: Mark Waugh, issakc-study@kc.issa.org, ISSA Education Committee Member For CISSP,

Chapter Membership Corner

The ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.

Top 10 Reasons Cybersecurity Professionals Join ISSA

- Build professional relationships
- Keep up on developments in information security/risk/privacy
- Content of chapter meetings
- Professional development or educational programming offerings
- Earn CPEs/CPUs
- Learn practical/best practices solutions
- Career information and employment opportunities
- Advance the profession
- Give back to the profession
- Develop the next generation of cybersecurity *professionals*

Contact: Wai Cheng, ISSA Director of Membership, Membership KC membership@kc.issa.org

For more information on member dues, http://www.issa.org/?page=MembershipDues

Webinars/Conferences

SAVE THE DATES:

- **INTERFACE - Kansas City**

July 12, 2018 | Overland Park Convention Center | 8:30am – 4:45pm

National Initiative for Cybersecurity Education (NICE):

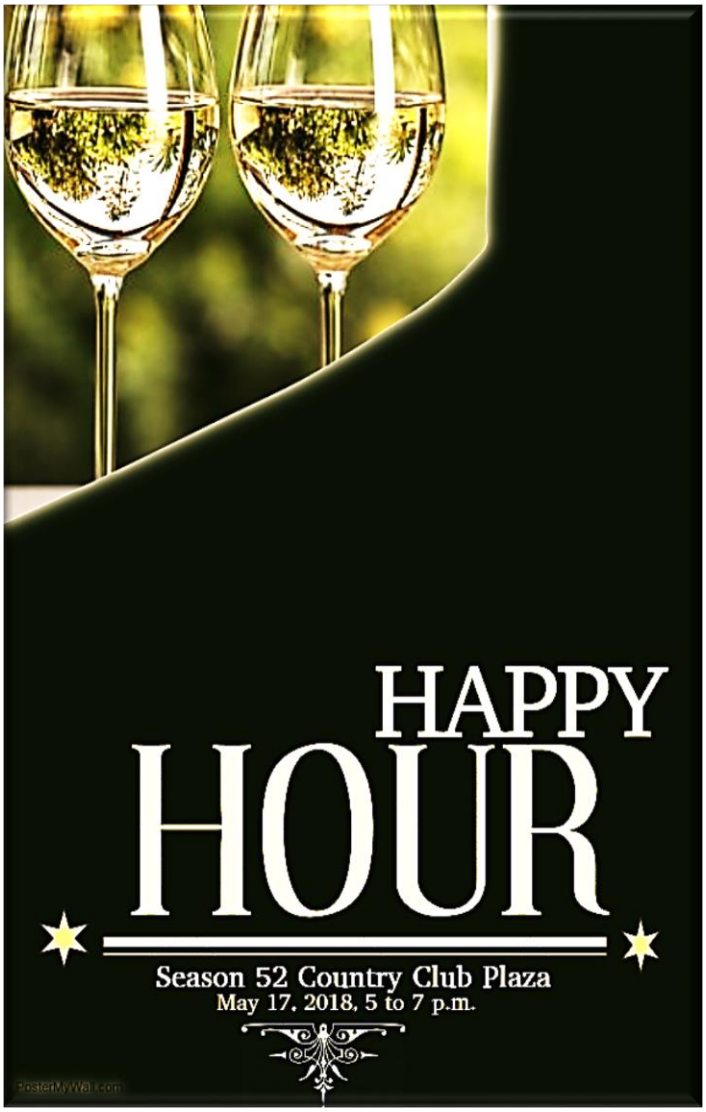
Preparing Students through Career and Technical Education and Cybersecurity Programs of Study

May 16, 2018 at 2:00pm ET

Career and Technical Education (CTE) programs are one of the most promising approaches to fast track students to enter the cybersecurity workforce. CTE provides students with cybersecurity-focused technical, academic, and employability skills through rigorous and applied coursework, work-based experiences, career and technical student organization leadership and competition experience, and industry-recognized certifications.

Registration space is limited. Learn more and RSVP at *nist.gov/nice/webinars*

ISSA HAPPY HOUR



Please join ISSA chapter members and other security professionals for Networking Affair/Happy Hour!

This networking affair/happy hour is held at Seasons 52 from 5:00 PM to 7:00 PM. The event is a great opportunity to become acquainted and interact with ISSA chapter members and other security professionals. Also, this special event is **FREE** for ISSA Kansas City chapter members!!! Guests and spouses are surely welcome to attend. All guests in attendance will receive two drink tickets.

Come along and join ISSA chapter members and other security professionals at Seasons 52 for a lively happy hour!

Date: Thursday, May17, 2018 from 5:00 PM to 7:00 PM

Location: Season 52
340 Ward Pkwy,
Kansas City, MO 64112
(816) 531-0052
http://www.seasons52.com/

Free for ISSA Members!!!
Cheers!
ISSA-Kansas City Chapter

rsvp@kc.issa.org

Register Now

ISSA-Kansas City May Chapter Event

On May 24, 2018 the ISSA-KC Chapter members, and other security professionals will hold a meeting Italy Restaurant in Kansas City, MO, to network and attend the monthly chapter meeting, with presentation topic

Speaker: David Swift, Securonix - Principal Architect, CISSP, GSEC, GCIH, GCIA, GSNA, ACTP. Mr. Swift is a leading security practitioner holding a variety of certifications including incident handling, intrusion analysis, and network auditing, has published multiple papers on SIEM, compliance and security strategies and has more than 25 years of experience. He joined Securonix in March of 2014, leaving a thriving SIEM practice at Accuvant that he led having completed over 300 SIEM projects covering nearly every industry leading product (HP/ArcSight, McAfee/Nitro, IBM/QRadar, Splunk….).

"At times I feel like a dinosaur having worked on computers since before the invention of the PC. But the firsthand experience on nearly every operating system, and hardware platform since the industry began comes in handy." (214) 724-7174 dswift@securonix.com,

Topic: Key Changes in Security and Why They Matter, AKA Data Swamps and Data Lakes

Location: Lidia's Italy Restaurant, 101 W. 22nd street, Kansas City, MO. 64108

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:
Pasta Tasting Trio - A sampling of three daily-made fresh and filled pastas.
Biscotti Platters - An assortment of house-made cookies & sweets to pass and share family style.

Soft drinks, Iced Tea, Coffee

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

Price:
$25.00 for ISSA Members,
$35.00 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

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
Wai Cheng
membership@kc.issa.org

Director of Education
Nicole Windholz
certification@kc.issa.org

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

Webmaster
Thomas Badgett
webmaster@kc.issa.org

Director of Marketing
Kristin Mehler
marketing@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney