ISACA®
Trust in, and value from, information systems
Greater Kansas City Chapter

March 2010 Volume 2, Issue 8

In this issue:

April Meeting Details

Practical Implementation of Automated Assessment Tools for the IT Auditor

IT auditors face significant challenges when performing deep technical assessments of networked information processing systems and devices. This meeting will be focused on illustrating how both commercially available and open source automated vulnerability and penetration testing tools can assist the IT Auditor in conducting an efficient and effective IT Audit.

Date: April 8, 2010

Time: 11:30 AM - 12:00 PM Registration | 12:00 - 1:00 PM Lunch | 1:00-3:00 PM Program

Location: Figlio's Tower | 209 West 46th Terrace | Kansas City | MO | 64112

Price: $35 members | $50 guests | $5 students

CPE: 2 Credits

Menu: TBD

Speaker: John Otte, Director, Strategic Services, Fishnet Security (bio on next page)

Board Elections

The Board members for the next year will be selected and announced during the May 2010 members meeting. If you are interested in being part of the Greater Kansas City ISACA Board, please contact Chapter President, Kevan Brewer at (816) 309-1202 or kevan_brewer@yahoo.com.

The elected positions are:
President
- Vice President
- Associate Vice President
- Treasurer
- Secretary

Registration is currently open on our website at http://www.isaca-kc.org/

Due to food and other costs incurred by ISACA, please contact us no later than the close of business of the Monday preceding the Thursday chapter meeting to cancel your registration. All late-cancellations and no-shows will still be charged the full meeting fee.

John A. Otte, Strategic Services

Summary

John is a seasoned Information Security and data protection professional with over 10 years of Systems Security Audit and controls experience. His vast experience includes over 20 years of Information Technology and engineering experience in the US Government, Department of Defense and the private sector. John's private sector experience includes assisting clients with assessments related to the Health Insurance Portability and Accountability Act

(HIPAA). John has extensive experience in the healthcare and public utility industries. John has lead both large and small health insurance companies, providers and hospitals with the assessment of their information processing

environments using the HIPAA privacy and security rules as the baseline. John has also performed a number of large engagements for companies that required experience in dealing with the National Institute of Health, The Center for Disease Control and the Center for Medicare/Medicaid. John's vast knowledge in Healthcare related issues and challenges enables him to provide cost effective pragmatic solutions to his clients.

John has extensive experience with assisting power and other public utility companies with the assessment of their compliance with the Northern American Electric Reliability Corporations (NERC) standards for Critical Infrastructure Protection (CIP). John has led several engagements for public utility companies to help them achieve and sustain compliance with these standards.

John has performed incident response and digital forensics work for a variety of commercial and government organizations. His investigation experience ranges from corporate misconduct to high profile criminal cases involving expert testimony. John is a national speaker on the topic of incident response and specializes in forensics cases related to the Payment Card Industry. Much of his recent expertise centers on IT governance and control. His knowledge in the Payment Card Industry Data Security Standards (PCI DSS) has assisted both medium and large organizations develop and implement comprehensive compliance programs. John has also helped organizations achieve high standards of governance and control by aiding in the implementation of leading IT governance frameworks such as ISO 17799.

John has assisted organizations with the implementation of leading Information Security standards and best practices within their IT environment. He has also conducted penetration and vulnerability studies for both Fortune 50 and Fortune 500 clients in the Midwest region. He has vast knowledge and experience with the selection and development of internal controls and utilizing corporate governance frameworks such as CoBIT, COSO and ISO 17799. John is also an avid speaker on information systems security topics at local chapters of Information Systems Security seminars and conferences.

Recent Projects

Eighth largest U.S. Telecom and Data Service Provider

John's experience with the classification, identification and categorization of data based on its value, sensitivity or context has proven invaluable to this client. This organization must comply with a myriad of regulatory acts and standards which makes data classification both comprehensive and complex. John's experience in the telecommunications industry coupled with his expertise in FCC and state Public Service Commission requirements enabled him to help

devise a data classification framework and strategy for this client. John's assistance with data classification resulted in an overall $2M in data storage savings to the client.

Fortune 500 Financial Services Institution

John provided critical trusted advisory services in the area of Data Loss Prevention to this global financial services client. Financial services organizations face very unique challenges in the area of data loss prevention. John's broad depth of knowledge and experience with a plethora of data loss prevention technologies enabled him to provide critical advice to reduce this clients overall risk of loss of data. John's knowledge of data loss prevention practices and strategies coupled with his keen business acumen enabled him to assist this organization with the prevention of loss of data totaling over 2.5 million dollars.

Fortune 500 Publishing Company, Des Moines, Iowa

John assisted this client with the assessment and remediation of this client's information systems and processing environment. The organization is subject to the provisions of the Payment Card Industry Data Security Standard and the Sarbanes-Oxley Act of 2002. The client faces many challenges regarding the processing and storage of credit card holder and other personally identifiable information. John's vast expertise and experience in the implementation of the PCI DSS and other information security best practices is proving to be invaluable to the client as this organization continues to strive to meet its PCI compliance objectives. As an information security master project planner and manager, John is consistently meeting the business and information technology goals while delivering quality security solutions on time and on budget.

Knowledge

- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation (NERC)
- Payment Card Industry compliance expertise and certification
- Regulatory compliance
- Enterprise Risk Management
- Incident response and Management
- Security Policy Review and Development
- Extensive network penetration testing, vulnerability testing and enterprise risk
- assessments
- Identity and Access Management
- Data loss prevention
- E-discovery
- Forensics
- Large-scale intrusion detection systems

Feedback Forum

If you have suggestions regarding presentation topics, speakers or locations, please contact BJ Smith, our Programs Chair.

2009 - 2010 Monthly Meeting

Sept. 10, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Securing Administrative Passwords" - Dave Adamczyk, Cyber-Ark
October 8, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	PCI and Privacy - Gleb Reznik, CISSP CISM PCI-QSA
November 12, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Hoodlums to Hackers – Jeff Lanza, former FBI Special Agent
December 10, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	*IT Vendor Audits* Bill McSpadden
January 14, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	*Virtualization Security* Michael T. Hoesing, University of Nebraska - Omaha
February 11, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	*Networking and Building Strong Professional Relationships* David Stroop, MHC Trucking
March 11, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	*Forensics* John Mallery, BKD
April 8, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	*Practical Implementation of Automated Assessment Tools for the IT Auditor* John Otte, Fishnet Security
May 13, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	*Top IT Infrastructure Security Threats* Dan Hirstein, Deloitte Annual Business Meeting

CISA and CISM Exams Information

The Certified Information Systems Auditor (CISA) is ISACA's cornerstone certification. The CISA certification has been earned by more than 60,000 professionals since inception and is for the IS audit, control, assurance and/or security professionals who wish to set themselves apart from their peers. Since 1978, the CISA certification has been renowned as the globally recognized achievement for those who control, monitor and assess an organization's information technology and business systems.

The Certified Information Security Manager (CISM) certification is a unique management focused certification that has been earned by over 9,000 professionals since its introduction in 2003. Unlike other security certifications, CISM is for the individual who manages, designs, oversees and assesses an enterprise's information security program. CISM defines the core competencies and international performance standards that those who have information security management responsibilities must master.

The IT Governance certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. More than 200 CGEIT certificates have been awarded. It is designed for professionals who have management, advisory, or assurance responsibilities as defined by a "job practice" consisting of IT governance related tasks and knowledge. Earning this designation will enable professionals to respond to the growing business demand for a comprehensive IT governance program that defines responsibility and accountability across the entire enterprise.

Upcoming Exams:

June 12th, 2010 CISA/CISM/CGEIT Exams Registration

- *April 7, 2010* - Final registration deadline for the June 12th, 2010 CISA/CISM/CGEIT exams.

Candidates are encouraged to register online through the International ISACA Web site and receive $50 off of the registration fee. Review materials (both written and review courses) may be purchased through ISACA as well.

CISA Certification Process:

Once you have passed the exam and have met the certification requirements (generally five years of systems audit or security experience, or allowable substitutions) as specified on the ISACA website, and then you will need to complete and submit the application for certification.

CISM Study Group Information:

No study group plans currently.

CGEIT Certification (Certified in the Governance of Enterprise IT):

ISACA's new IT Governance certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. For further information, please visit the Official ISACA International website: CGEIT Certification Details.

Knowledge Base

Did you know as an ISACA member, you have the opportunity to attend e-symposiums and earn CPE credits ***free of charge***?

Visit http://isaca.brighttalk.com/ to learn more about e-symposiums.

CPEs!!

Continue your education with ISACA by visiting the International ISACA website at http://www.isaca.org or the location website at http://www.isaca-kc.org

More information to come in the future newsletter with CPE options.

Upcoming Events from ISACA—International

ISACA Training Week

Presented by ISACA®, Training Week provides a unique educational experience.

The Training Week courses use a combination of lecture, case study, class discussion and group exercises to explore all the nuances and subtleties of the named topics. Training Week participants will learn about proven strategies and techniques based upon best practices and lessons learned from the ISACA community.

Network Security Conference

ISACA's Network Security Conference is uniquely designed to meet the education and training needs of the seasoned IT practitioner as well as the newcomer. Whether you are an experienced information security professional keeping pace with complex network environments, an IS auditor looking to gain detailed knowledge and competencies on specific topics, an IS control professional seeking information on guarding one of your organization's most important assets or otherwise involved with information security, this year's Network Security Conference will benefit you.

Information Security Management Conference

Strategic vision for information security managers

ISACA® is pleased to announce its fourth annual Information Security Management Conference, designed for experienced information security managers and those who have information security management responsibilities. The event will feature a variety of sessions dealing with information security managerial issues and information security programme issues. The combination of management focus and highly detailed content will provide the attendee with an opportunity to customize the conference experience to his/her specific interests and professional needs. Experienced professionals as well as new or aspiring Certified Information Security Manager® (CISM®) holders will find great value in the conference.

Visit http://www.isaca.org for more details on each event.

Feedback Forum

If you have any suggestions regarding newsletter content or formatting, please contact our Newsletter Editor,: Email: urvi.biyala@ey.com.

2009 - 2010 Board Members

NAME	COMPANY	BOARD POSITION	EMAIL
Jim Wilcox	American Century	Director	jim_wilcox@americancentury.com
Jennifer Harper	AIPC	Director	jharper@aipc.com
Alfie Mahmoud	KPMG	Director	amahmoud@kpmg.com
Kevan Brewer	eSolution Technologies	President	kevan_brewer@yahoo.com
Jerry Wistrand	Commerce Bank	Vice President / CISA Review	Gerald.Wistrand@Commercebank.com
Nila Henderson	CenturyLink	Treasurer / Webmaster	Nila.K.Henderson@embarq.com
Wendy Dobratz	NAIC	Secretary	wevans@naic.org
BJ Smith	DST Systems	Programs Committee Chair	'BJSmith@dstsystems.com
Reed Anderson	CenturyLink	Programs Committee	Reed.Anderson@Embarq.com
Matt Suozzo	Protiviti	Membership	Matt.Suozzo@protiviti.com
Urvi Biyala	Ernst & Young	Newsletter Editor	Urvi.Biyala@ey.com