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

Ethical Hacking – Making it More than Something That's Done To You

Date: April 10th, 2014

Time: 11:30 Registration | 12:00 - 1:00 PM Lunch | 1:00 PM –3:00 PM Presentation

Location: Ritz Charles | 9000 West 137th Street | Overland Park, KS 66221

CPE's: 2 Credits

**Please note actual CPE hours granted are dependent upon duration of speaker's presentation and may differ from advertised number of CPE hours.*

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

Menu: Salad: Mixed Tossed Green Salad | Entrée: Apple Jack Turkey | Vegetable: Julienne Vegetable Saute | Starch: Garlic Mashed Potatoes | Dessert: Ice Cream Brownie Sundae

Please denote any dietary restrictions when registering and accommodations will be made.

Speaker Summaries:

Bob Cheripka, CISSP, LTC, USA (Ret).

Bob is a Manager in Deloitte & Touche LLP's Cyber Risk Services and has been with the organization for over three years, coming to Deloitte with over 12 years of experience in computer network defense operations and over 5 years of intelligence operations, while working for the United States Army. Bob's experience includes Information Security/Assurance Planning and Implementation, Public Key Infrastructure Program Implementation, Watch Center Operations , Security Assessments and Penetration Testing, Crisis Action Team Planning, Cyber Threat Intelligence, and Defense Program Development and Implementation. Bob has a Master's Degree in Information Resource Management from Central Michigan University and holds various Cyber Security Certifications.

Bob's hobbies including brewing, hunting, and participating in Medieval Re-Enactments

Ian Barton

Ian Barton joined Deloitte as a Cyber Risk Services Consultant in August 2012. He joined Deloitte as a campus hire from Texas A&M University, where he majored in Management Information Systems. Prior to Deloitte, he interned with McAfee as a Global Information Security Services Analyst and VendorSafe Technologies as a Lead NOC Analyst. He holds the GIAC Certified Forensic Examiner (GCFE) certification, and is an Associate of (ISC)2 towards the CISSP. His passion lies in Cyber Incident Response and Security Process Development.

When not on the clock, you can find Ian tinkering with a variety of hobbyist electronics including Quadcopters, Raspberry Pi's, and other electronic projects.

Presentation Overview:

As the security landscape continues to evolve, almost on a daily basis, security professionals are in a constant competition between threats, risks, resources, and time to try to protect the crown jewels of their organization. Ethical Hacking presents a unique capability to strengthen and bolster an organization's security capabilities if it is employed in the proper manner. All too often, ethical hacking (also known as Attack and Penetration Testing) is viewed as something that is done to an organization's security department in order to evaluate performance. This limited view of Ethical Hacking limits the true value of this capability. This presentation will explore an alternative view of ethical hacking by first looking at the Changing Threat Landscape & the implications for the role of Security Control Testing & Audits in keeping an organization secure, vigilant, and resilient. We will then explore what is Ethical Hacking and why should we care about it, focusing on how Ethical Hacking and Diagnostic Services should fit into security organization's capabilities. We will then dig even deeper and look specifically at Ethical Hacking in Support of Security (i.e., the Adversaries View of My Security Controls) and Ethical Hacking in Support of Audits. The presentation will wrap up with a discussion on specific considerations & risks in planning Ethical Hacking and ways to successfully integrate Ethical Hacking & Diagnostic Service into Assessments & Audits.