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 following pages)

John A. Otte, Director, 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

Certifications

- CISSP
- CISA
- ISO 27001 Lead Auditor
- PCI QSA

Technical Computing Environments

- Client/server, local area networks
- Wide area networks
- UNIX
- Enterprise class routers and switches
- Databases (Oracle, SQL, Informix and DB2)
- Enterprise-level firewalls