

WHO SHOULD ATTEND

This symposium is designed for anyone practicing or interested in information systems risk, security and assurance. It is especially geared toward professionals who supervise information systems departments, CIOs, CITP's, assurance service providers such as auditors in CPA firms who wish to learn more about information systems security, Information Systems Auditors, Internal Auditors, college professors who teach information systems, members of professional organizations such as the AICPA, OSCP, IIA, IMA, ISACA and employees of local, state, and federal governments with responsibility for information systems.

THE PROGRAM

- 7:30 - 8:00** **Registration & Continental Breakfast**
- 8:00 - 8:30** **Welcome**
- 8:30 - 10:00** **Information Security & Global Information Flows**
D. Timothy Hartzell
- 10:00 - 10:15** **Refreshment Break**
- 10:15 - 12:00** **Cyber Crime and Digital Evidence Protection**
Edward L. Goings
- 12:00 - 1:15** **Lunch**
- 1:15 - 3:00** **Biometrics and Authentication**
Mark R. Herbst and Timothy W. Morgan
- 3:00 - 3:15** **Refreshment Break**
- 3:15 - 5:00** **Security Best Practices**
Dr. Ron Ross

Please Return With Payment Payable to The University of Akron

Registration
2004 Symposium on Information Systems Risks, Security, & Assurance

Please print:

Name(s): _____
 Company Name: _____
 Address: _____
 Zip: _____

Number of people attending at \$175 (\$200 if paid at the door) ISACA OSCP IMA College Professor

Number of people attending at \$200 (\$225 if paid at the door) _____
 Number of Vegetarian Meals: _____

Total Enclosed _____

Return with check payable to School of Accountancy, University of Akron by February 20, 2004 to:

Terri Brunson
 The George W. Davenport School of Accountancy
 The University of Akron
 Akron, Ohio 44325-4802
 (330) 972-6233 (phone)
 (330) 972-8597 (fax)
 E-mail: cretisa@uakron.edu
<http://www3.uakron.edu/cba/cretisa>

Bulk Rate
Permit



College of
Business
Administration

**SECOND ANNUAL
SYMPOSIUM ON
INFORMATION
SYSTEMS RISK,
SECURITY & ASSURANCE**

**FRIDAY, FEBRUARY 27, 2004
7:30 AM – 5:00 PM**

This year's theme:
**INFORMATION SECURITY &
ENTERPRISE RISK**

CPE Credit: 8 hours

LOCATION
 Crowne Plaza at Quaker Square
 Downtown Akron
 135 South Broadway Street
 Akron, OH 44304
 (330) 253-5970

SPONSORED BY

- ◆ The Ohio Society of Certified Public Accountants
- ◆ Information Systems Audit & Control Association—North East Ohio Chapter
- ◆ Institute of Management Accountants—Akron Chapter
- ◆ Institute of Internal Auditors—Akron Chapter
- ◆ Course Technology

THE SESSIONS

Information Security and Global Information Flows **D. Timothy Hartzell, CISSP, CISM**

Information systems managers have been hit with a deluge of security and privacy regulations. Everything from encrypting credit card numbers to guaranteeing the privacy of personal financial information, as governed by the Gramm Leach Bliley Act (GLBA), has put added importance on properly securing their systems. Some regulations have been moving targets. The Health Information Portability and Accountability Act (HIPAA) was enacted in 1996, yet all regulations have not yet been finalized. This session will discuss the aspects of security and privacy regulations and look at the unique challenges presented by global information flows.

Tim Hartzell is a Senior Manager in the Technology Risk Consulting practice at Protiviti, Inc. and leads the Information Security practice for the Ohio and Western Pa. area. Tim has more than twenty-five years of experience in various aspects of information technologies and has taught courses in telecommunication and networking at Point Park University in Pittsburgh. For the past six years he has worked exclusively in the Information Systems Security field in the Financial Services, Manufacturing, and Health Care industries. Tim holds a BS in Electrical Engineering Technology and an MBA.

Cyber Crime and Digital Evidence Protection **Edward L. Goings**

This session will provide information on techniques and services to investigate cyber crimes including techniques to discover, recover and present digital evidence. Attendees will learn the do's and don'ts of dealing with digital evidence so that the results stand up in court. Can your competition steal your proprietary intellectual property and trade secrets from under your very nose? They can, and this case study shows you how it happened in one real world example. Only the names have been changed to "protect the innocent". This case study discusses the facts around an employee using a Trojan horse virus and his company's corporate intranet to steal sensitive information from executive officers' computers, and then e-mailing it to a competitor in exchange for a payoff and a promise of a future job. The topic involves IP damages, steganography (used by the terrorists to communicate), digital watermarking, electronic discovery, and other timely subjects.

Ed Goings is a Manager in KPMG LLP's Forensic Technology Services Practice based in Chicago, IL. Ed is tasked with providing Digital Evidence Recovery and Forensic Data Analysis services nationally but focuses on the Midwest market. Ed has thirteen years of active duty military service during which he served as a Federal Agent in Computer Crime Investigations with the United States Air Force Office of Special Investigations. During his career, Ed has conducted computer intrusion investigations for the United States Air Force, conducted hundreds of Computer Forensic examinations on electronic stored data for the purpose of evidence preservation and admissibility in court, and has testified numerous times in Federal Court on electronic evidence. Further, Ed was tasked to identify how and where intruders potentially access computer systems and then collect pertinent evidence to assist in prosecuting the perpetrator. Ed has provided valuable information to Air Force System Administrator on computer systems' vulnerabilities and network security.

Biometrics and Authentication **Mark R. Herbst & Timothy W. Morgan**

This two-part session focuses on Biometrics within the Department of Defense (DoD). The first portion will be an overview of biometrics and will introduce the DoD's Biometrics Management Program and the activities at the DoD Biometrics Fusion Center. This will include the DoD's changing security requirements and how the DoD is using biometric solutions to meet those requirements. The second segment will discuss the role of biometrics in the authentication process and show the benefits and shortcomings of the various biometric technologies. There will also be a synopsis of major advances in the biometric marketplace and some of the latest biometric security trends.

Mark R. Herbst is a Senior Biometric Test Engineer for the West Virginia High Technology Consortium Foundation, working at the Department of Defense Biometrics Fusion Center (BFC) in Bridgeport, West Virginia. He is responsible for the quality of all BFC test reports and assists in the development of test processes and procedures.

Timothy W. Morgan is a Project Manager with Information Systems Support, working at the Department of Defense Biometrics Fusion Center (BFC) in Bridgeport, West Virginia. He currently manages biometrics research liaison programs. Tim has managed programs for the Navy Supply Systems Command and the Institute for Scientific Research in the areas of Finance and Logistics, Operations Research, and Test and Evaluation.

Security Best Practices **Dr. Ron Ross**

This session will present the National Institute of Standards and Technology (NIST) strategy for developing security standards and guidelines mandated by the Federal Information Security Management Act (FISMA) of 2002. Three key documents will be discussed: Federal Information Processing Standard Publication 199, *Standards for the Security Categorization of Federal Information and Information Systems*; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*; and NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. The use of the new security standards and guidelines in developing effective organization-wide information security programs and ultimately achieving more secure enterprise information systems for the nation's critical information infrastructure will also be discussed. Web-based information security resources will be available to assist organizations in all aspects of securing their enterprise information systems. NIST information security programs and security-related information can be accessed by visiting the Computer Security Division web site at: <http://csrc.nist.gov>.

Dr. Ron Ross, a graduate of the United States Military Academy at West Point, is a senior computer scientist and information security researcher at the National Institute of Standards and Technology (NIST). His current areas of specialization include security testing and evaluation, security requirements definition, and information assurance. For the past five years, Dr. Ross has served as the Director of the National Information Assurance Partnership, a joint activity of NIST and the National Security Agency. Dr. Ross is a graduate of the Program Management School at the Defense Systems Management College and holds both Masters and Ph.D. degrees in Computer Science from the United States Naval Postgraduate School.

FEEDBACK FROM LAST YEAR'S ATTENDEES

Attendees to last year's Symposium gave resoundingly high satisfaction ratings to the speakers and topics. They indicated solid support to continue the event annually and to lend their encouragement for others to attend.

When asked to make additional comments, here is what attendees had to say:

- ▣ Keep it the way it is!
- ▣ Excellent Program
- ▣ Topics very relevant
- ▣ Very informative
- ▣ The location was easy to find and quite convenient

HOSTED BY

The G. W. Daverio School of Accountancy
College of Business Administration
The University of Akron
Akron, OH 44325-4802
(330) 972-7588 (phone)
(330) 972-8597 (fax)

For More Information Visit: <http://www3.uakron.edu/cba/cretisa>

CONTINUING EDUCATION CREDIT

CPE Credit: Attendees qualify for 8.0 hours of credit. Fields of study: Consulting; Internal Controls, and Risk Assessment. Level of knowledge: Intermediate. Teaching Method: Seminar/Lecture. You will receive a professionally prepared manual compiled by the faculty involved with the symposium.

Continental breakfast, lunch, and snacks will be provided during the symposium. The fee for members of Sponsoring Organizations and college professors is \$175 when paid by February 20, 2004 (\$200, thereafter). For all others, the fee is \$200 when paid by February 20, 2004 (\$225, thereafter).