

September 16, 17 & 18, 2009, Toronto

7th

Reinventing the Chief Security Officer

The Latest Innovations in Corporate Security Practices

"I found the real life stories from other companies very valuable. It wasn't just lots of theory, it was real people and real solutions."

"Well-rounded and well-balanced presentations - a good cross-section of security professionals - great learning environment."

"Good networking and contact building."

"Very thought provoking."

Participating organizations

AFI INTERNATIONAL GROUP INC.
BRUCE POWER
CADILLAC FAIRVIEW CORPORATION LIMITED
CANADA'S WONDERLAND
CANADIAN ARMED ROBBERY TRAINING ASSOCIATES INC. (CARTA INC.)
CARA OPERATIONS LIMITED
CITY OF TORONTO
DANIER LEATHER INC.
DUFFERIN-PEEL CATHOLIC DISTRICT SCHOOL BOARD
IMPERIAL OIL LTD.
MCLEAN SECURITY ADVISORY & ASSOCIATES INC.
M.D. BURGESS AND ASSOCIATES INC.
MG FORENSIC ACCOUNTING & INVESTIGATIONS INC.
PARAGON PROTECTION LIMITED
PRICEWATERHOUSECOOPERS LLP
SAFEGUARD SECURITY & INVESTIGATION SERVICES LTD.
VPI EMPLOYMENT SERVICES
WOODBINE ENTERTAINMENT GROUP

Optional workshops

PSISA: THE NEW REALITY - TRAINING AND DUE DILIGENCE IN A COST EFFECTIVE AND COMPETITIVE MARKET

Mike Burgess, President and Managing Director,
M.D. Burgess and Associates Inc.

FACILITY ASSESSMENTS

Graeme Eastmure, Executive Vice President, Operations,
Safeguard Security & Investigation Services Ltd.

Conference highlights

- Maximizing the effectiveness of security practices in the face of limited resources and budget cutbacks
- Rethinking security spending to be more proactive and innovative
- Discover how to align security with strategic business objectives
- Learn how to master the risk/reward equation and adapt to the changing nature of risk
- Uncover the latest innovative security tools and practices
- Understand the nature and probability of catastrophic and significant security risk events in today's world
- Examine best practices and methods for training and evaluating employees in light of the new PSISA training requirements
- Hear about leading practices for preparing for and dealing with labour disputes
- Learn strategies for protecting the critical infrastructure of our communities
- Discover the latest technological options available for increasing security measures





SESSION 1

LINKING STRATEGY TO BUSINESS GOALS

Gene McLean, Principal,
McLean Security Advisory & Associates Inc.

Wednesday, September 16th

9:00-9:45

EXECUTIVE PROTECTION

Myron Zukewich, Security Analyst, Imperial Oil Ltd.

The threats facing an executive vary widely depending on the size of the company, the industry it belongs to and the individual executive's profile. Protecting an individual is very different from securing a facility, so CSOs put in charge of executive protection programs must find the balance of protecting their company's assets while making the security practices palatable to the executives who are impacted by it. This session will examine the steps in designing and implementing a comprehensive executive and employee protection plan.

- Conducting a comprehensive site survey
- Leading threats to executives
- Protective measures: home security systems, bodyguards, armored vehicles and vehicle scramble plans, mail screening, private jet travel, background checks for other employees, and other precautions
- Providing security for immediate and/or extended family members to prevent kidnapping and extortion

9:45-10:30

CASE STUDY: TRAINING AND EVALUATING YOUR SECURITY STAFF IN A HIGH RISK ENVIRONMENT

Frank Saunders, Vice President of Safety and Environment, Bruce Power

With its claim of making "Safety First" its number one value, Bruce Power has always measured itself against world-class standards. Understanding that safety is a key to commercial success, they have strove to not only ensure the nuclear safety of its generating stations, but also the safety of its employees and the surrounding communities. In response to the Private Security and Investigative Services Act, which sets out new and stricter standards and training requirements, Bruce Power has adopted a number of initiatives to meet these standards. This case study will examine Bruce Power's award winning security practices.

- Bruce Power safety initiatives
- Target Zero: an employee-driven initiative developed by a coalition of management and union representatives to achieve zero industrial accidents or occupational illnesses on site
- The implementation of the International Safety Rating System
- Becoming ISO 14001 registered
- The introduction of the Safety Supervisory Board
- Encouraging all staff to become involved in safety initiatives
- Upgrades to security systems

10:30-11:00 NETWORKING BREAK

11:00-11:45

ONE LESSON LEARNED FROM CONVERGENCE: SECURITY METRICS

Jim Maddin, Security Manager, Canada's Wonderland

It has been the recent widely held belief amongst security people that companies need to move towards a convergence of traditional, electronic and IT security to reduce risk, mitigate disaster and support business objectives. The convergence of physical and information security has been trumpeted as the next big thing in security. But while it is easy to see why there has been a convergence, the shift rarely occurs without some difficulties. This is happening at a time when the use of metrics in the security field is still in its infancy, even though there are excellent resources available to assist security personnel in gathering and assessing data. This session will examine the results to date for companies adopting a convergence strategy.

- Computer metrics as a model for security metrics
- The effective use of metrics and dashboards
- Lessons learned from the move to convergence: recent experiences implementing converged security plans
- Effective use of computer systems to enhance company security
- The difficulty and practicality of merging two very different cultures: security vs. IT

11:45-12:30

PANEL DISCUSSION: LINKING SECURITY AND BUSINESS STRATEGY

David M. Hyde, Director, Security Services, Cadillac Fairview Corporation Limited
Victor Chu, Director iT Operations, Cara Operations Limited
Dwayne Nichol, Director of Security, City of Toronto
Myron Zukewich, Security Analyst, Imperial Oil Ltd.
Gene McLean, Principal, McLean Security Advisory & Associates Inc.

In today's era of economic hardship and mounting security threats, the responsibility to protect employees and organizational assets, while always a concern, has become a main priority and challenge to businesses. In these difficult times, with the mission of security expanding, one of the main responsibilities of a CSO is to develop and implement an effective security strategy that must not only convey an understanding of the nature and probability of significant security risk events facing an organization but must also be linked to its overall business strategy. This panel discussion will examine the issues involved in formulating and implementing a security strategy that will complement your business strategy.

- Developing and implementing a security master plan
- Ensuring plan is consistent with company's overall business plan
- Installing elements of a security program and processes throughout the organization
- Communicating the strategy, costs and related impacts to the highest levels of the organization

12:30-1:30 LUNCH

LINKING SECURITY & BUSINESS STRATEGY - EMERGING THREATS



SESSION 2

SECURITY THREATS

Dwaine Nichol, Director of Security,
City of Toronto

Wednesday, September 16th

1:30-2:15

THREAT & RISK ASSESSMENTS: BEST PRACTICES

Dwaine Nichol, Director Of Security, City of Toronto

Assessing external and internal security threats and providing a plan to mitigate risk is critical for the protection of corporate personnel and assets. Threat and risk assessments, which serve to identify indicators of future activity and predict the probability of the occurrence of such events and their impact on business, should be performed on a priority basis for all facets of an organization to ensure that baseline security standards are current and evergreen. Topics to be examined include:

- Assessing and defining security's current and future role in your organization
- Analyzing the gap between where your organization's security capabilities are and where they need to be
- Identifying capability gaps, checking current project alignment, determining the appropriate size of a reasonable investment and identifying where your organization should be committing its scarce resources
- What is the value gained from assessments?
- Risk mitigation approaches
- Importance of achieving executive buy-in

2:15-3:00

CREATING A DYNAMIC SECURITY DEPARTMENT: LEADERSHIP IN DIFFICULT TIMES

Kevin Murphy, Director, Security Operations, Woodbine Entertainment Group

The ever-increasing demands on security departments come at a time when they are often facing limited resources and the threat of budget cuts as many businesses are struggling simply to survive in this economy. Doing more with less and meeting escalating expectations while retaining the best employees are a daily reality for today's top security professionals. Success requires leadership and vision. These attributes are critical and will not only ensure your success but also the success of your team and your organization.

- Understanding the mission, objectives and values of your organization
- Developing a metrics approach: use of risk analysis metrics and benchmarks
- Demonstrating the value of your ideas using metrics and return on security investments
- Defining the competencies and styles of leadership
- Comparing leadership vs. management
- How to establish effective communication and motivation
- How to grow a team: continually improving the competencies of you and your team
- Setting goals and direction

3:00-3:30 NETWORKING BREAK

3:30-4:15

ROBBERY MITIGATION AND MANAGEMENT

Todd Moore, President, Canadian Armed Robbery Training Associates Inc. (CARTA Inc.)

For today's CSO, the spectre of armed robbery may be overshadowed by the growing threat of fraud schemes and attacks on information systems, but robbery can have a substantial impact on the business bottom line. A CSO must be mindful that robbery is a personal crime and the traumatic effects suffered by employees can be devastating, regardless of the amount stolen. While businesses tend to focus primarily on physical security to deter robbery, many are ill-prepared when the deterrents fail and the onus falls on employees to properly manage a robbery situation. Robbery training is an essential component of ensuring employee safety. This session will discuss:

- Liability issues surrounding armed robberies
- Understanding the robber's goals and motives
- Robbery trends: financial vs. commercial
- Dispelling the myths associated with armed robbery
- Types of resistance
- Observation skills
- Post-robbery procedures

4:15-5:00

PRIVACY IN THE WORKPLACE

J. Curtis McDonnell, General Counsel, vpi Employment Services

Privacy legislation in Canada confers extensive rights on individuals to control the collection, use and disclosure of personal information, including the right to privacy of workers. As a result, finding the right balance between privacy and security in the workplace has become an increasingly difficult task, particularly since the notion of personal information has been expanding recently. This presentation will examine the ways in which privacy laws carry implications for workplace security.

- Surveillance and biometric authentication of employees and others from a Canadian legal perspective
- Legal and legislative guidelines with respect to privacy breaches
- Privacy expectations for network transmissions, wireless devices, internal data storage, archive storage and remote or portable PCs
- Privacy and the use of CCTVs
- Privacy issues when conducting investigations

INFORMATION SECURITY RISKS - PSISA TRAINING REQUIREMENTS



SESSION 3

ENTERPRISE SECURITY ARCHITECTURE

Alvaro J. Orrantia, MBA, CISSP, CBCP, Advisory Services, Performance Improvement & Risk, PricewaterhouseCoopers LLP

Thursday, September 17th

9:00-9:45

EFFECTIVE RESPONSES TO CRITICAL INCIDENTS

*Minaz Jivraj, Chief Security Officer,
Dufferin-Peel Catholic District School Board*

Columbine, Dawson College, Ecole Polytechnique – even the mere mention of these incidents evoke horror and trepidation. For the chief security officer, they are also a challenge and unfortunately, can be part of the job. While it is virtually impossible to anticipate and prevent such incidents, as can be seen by the increase in the number of workplace shootings by disgruntled employees, lessons have been learned from those that have occurred to help CSOs determine best practices for responding to such critical incidents in order to minimize loss of life, injury and damage. This presentation will touch on:

- Learning from the past: how history dictates solutions for future incidents
- Maximizing safety, particularly in the school setting
- Planning and organizing an effective response plan for your organization
- Responding effectively to critical incidents and managing the outcome of the incident

9:45-10:30

MANAGING INFORMATION SECURITY RISK: DEVELOPING AN INFORMATION SECURITY PROGRAM

*Alvaro J. Orrantia, MBA, CISSP, CBCP, Advisory Services,
Performance Improvement & Risk, PricewaterhouseCoopers LLP*

With the increasing threat of information security breaches and identity theft, as well as the growing complexity of corporate networks and increased legal liability, CSOs must work harder than ever to protect corporate data from both external and internal threats. An information security program defines how business objectives translate into information security controls. It is a set of policies, processes, people and resources aligned to make these controls operate effectively to protect the business and dynamically adapt to changing conditions. This session will look at how to manage information security risks through the development of an information security program.

- Establishing and managing an information security program
- Components of a comprehensive plan: prevention, detection, response
- Developing an enterprise security architecture
- Security program processes: design/development, monitoring, administration
- Protecting information assets: confidentiality, integrity, availability
- Translating business drivers, regulatory control objectives and audit issues into actionable plans

10:30-11:00 NETWORKING BREAK

11:00-11:45

ESTABLISHING INTERNAL INVESTIGATION GUIDELINES: INCORPORATING THE LATEST INVESTIGATIVE STRATEGIES AND TECHNIQUES

*Stephen K. McIntyre, President,
MG Forensic Accounting & Investigations Inc.*

Fraud, employee theft, dodgy financial schemes and violence in the workplace - there is only one thing worse than corruption and wrongdoing within your organization, and that is botching the ensuing investigation and leaving the company vulnerable to further loss, reputation damage and litigation. There are several reasons why some workplace investigations are not as successful as others, but one of the greatest contributors to failure is that many investigators leap into investigations without adequate procedures and guidelines in place. This discussion will focus on strategies for establishing successful internal investigation guidelines incorporating the latest investigative strategies and techniques

- How to begin writing your organization's internal investigation guidelines
- Ensuring employee conduct policies are in place and understood by all
- Essential qualities associated with successful investigations that should be incorporated into the guidelines
- Establishing guidelines and procedures for the interview process
- Developing safe guidelines for employees to report suspect behaviour
- New investigative strategies and techniques

11:45-12:30

USING IN-HOUSE TRAINERS/TRAINING PROGRAMS TO INCREASE COST EFFECTIVENESS UNDER THE NEW MANDATORY REGULATIONS

*Mike Burgess, President and Managing Director,
M.D. Burgess and Associates*

As part of the licensing requirements of the Private Security and Investigative Services Act, security personnel and private investigators will be required to have yearly training in such areas as legal awareness, offences, behaviour management, handcuffing and searching procedures. The testing and training components were supposed to take effect in November 2008, but have been delayed to this year. This session will examine the benefits and challenges of establishing and managing an in-house training program for security personnel.

- Applying to the Ministry to have certified in-house trainers and programs
- The process of establishing an in-house training program
- Retaining qualified in-house trainers
- Required elements of an in-house training program
- Advantages of using in-house trainers: potential cost savings
- Meeting the PSISA training requirements

12:30-1:30 LUNCH

TECHNOLOGICAL ADVANCES - FACILITY SECURITIZATION



SESSION 4

ENTERPRISE SECURITY ARCHITECTURE

Michael W. Fenton, Director of Consulting & Support Services,
Paragon Protection Limited

Thursday, September 17th

1:30-2:15

LOSS PREVENTION & SECURITY IN THE RETAIL INDUSTRY

Steve Waldron, Director, Loss Prevention, Danier Leather Inc.

In today's economic environment, where retailers are fighting to maintain revenues and profitability, every retail company is vulnerable to a wide array of crimes such as shoplifting, package pilferage, employee theft, embezzlement, credit fraud and check fraud. In spite of the size of the threat, many retailers are still unsuccessful in creating effective loss prevention techniques. This session will examine the latest best practices for loss prevention and security techniques for the retail industry.

- Forms of employee theft and how to combat it:
cash theft, ringing up fake gift cards, passing merchandise, theft of merchandise, discount and commission fraud
- Credit card theft
- Cheque fraud
- Margin loss and sweethearting
- The latest equipment, tactics and technology employed in loss prevention: camera systems; electronic article surveillance, two-way radio sets, audits and reporting; ink tags, ceiling mirrors, consent searches, viewing towers
- Training of loss prevention personnel

2:15-3:00

LAPTOP THEFT: PHYSICAL, PROCEDURAL AND TECHNOLOGICAL SOLUTIONS

Michael W. Fenton, Director of Consulting & Support Services, Paragon Protection Limited

Though there are many methods to prevent the theft of laptop computers and protect the data they contain, laptop theft remains a growing threat. The seriousness of this threat stems from the fact that it does not only involve the loss of the hardware itself but also potentially sensitive data and personal information. This session will examine the ever-present threat of laptop theft, including a statistical review, re-victimization rates and a broad spectrum of countermeasures.

- Proper security precautions to protect personal bookkeeping files, documents containing passwords, addresses, employee and customer information
- Inside protection: full disk encryption, remote laptop security
- Inadequacy of reliance on passwords
- Traveling with a laptop
- Technological solutions: motion sensors and alarms
- Proactive safety training for employees
- Providing employees with adequate secure storage areas for their laptops
- Keeping an inventory of all company owned laptops and computers
- Use of removable hard drives carried separately from the laptop

3:00-3:30 NETWORKING BREAK

3:30-4:15

FACILITY SECURITIZATION: TECHNOLOGICAL ADVANCES

Graeme Eastmure, Executive Vice President, Operations, Safeguard Security & Investigation Services Ltd.

To shore up the security of your facilities in the face of threats such as those presented by disgruntled employees, domestic or international terrorism, identity theft and data theft, a CSO must consider all tools at their disposal. The CSO must work with facility managers and security personnel using the latest tools and strategies to present a unified approach to safeguarding their organization. This session will look at best practices for securing your facilities.

- Conducting vulnerability assessments: assess internal and external threats that could affect employees and company assets
- IP-based CCTVs: establishing security goals for CCTV and design considerations
- Alarm system
- Sensors and intrusion detection
- Key and lock control
- Access control: advantages and disadvantages of various access control technologies
- Cost-effective security solutions that fall in line with the company's business objectives
- Perimeter protection including parking lots and areas outside buildings

4:15-5:00

MAINTAINING SECURITY DURING A LABOUR DISPUTE

Peter Martin, Chief Operating Officer for North America, AFI International Group Inc.

A properly developed advance strike plan is the best way to tackle the issue of security during a labour dispute. Emotions can run high once a work action begins - and that is no time to develop security processes, as post-dispute relations can be permanently harmed. This presentation will focus on leading practices for preparing for and dealing with labour disputes.

- Developing a labour strike contingency plan
- Working toward a positive post-dispute relationship
- Key security tools and procedures that benefit all sides
- Protecting your company from irreparable damage and lawsuits
- Preparation: the key to success in surviving a labour dispute
- Ensuring security in operations of critical infrastructure during a strike

OPTIONAL WORKSHOP A

Friday, September 18th - 9:00-noon



PSISA: THE NEW REALITY - TRAINING AND DUE DILIGENCE IN A COST EFFECTIVE AND COMPETITIVE MARKET

Mike Burgess, President and Managing Director, M.D. Burgess and Associates Inc.

The Private Security and Investigative Services Act (PSISA), which requires all private security practitioners, including in-house security staff, to be licensed, is causing many security professionals to re-examine their workforce regarding how they train and prepare officers for licensing. The Act attempts to ensure that security personnel have all the necessary resources and training they need, as the law sets out new and stricter standards and training requirements and regulates the type of uniforms, equipment and vehicles that can be used by private security personnel. The Act does not only significantly alter the way in which all Ontario security officers govern themselves and the way in which employers train, instruct and monitor staff, but it also has the potential of creating a trap for those employers who fail to understand and implement its requirements or who fail to closely monitor both their own security staff and those of firms with whom they contract for services. This interactive workshop will examine the impact of PSISA with a focus on training and due diligence practices.

- How to prove due diligence and be properly prepared while staying within budgets
- Alternative training methods and tactics that will increase the skills, knowledge and abilities of front-line officers while being cost-effective
- How to seek out the expertise you need, verify the credentials of subcontractors and obtain trainer qualifications
- Registering with the Ministry's Private Security and Investigative Services Branch
- Regulation of the type of uniforms, equipment and vehicles that can be used by private security personnel
- Mandatory training requirement for various categories of licensed personnel under PSISA
- Training and testing standards: competencies and examinations for applicants and current license holders
- Binding Code of Conduct on the security industry
- Training as a prerequisite to licensing

Mike Burgess is the President and Managing Director of M.D. Burgess and Associates Inc., a training network formed specifically to train people in the area of dealing with difficult people and violence prevention. He is a recognized expert in the use of force and dealing with violence in various workplaces. The company is based in Southern Ontario and facilitates programs and training worldwide.

OPTIONAL WORKSHOP B

Friday, September 18th - 1:30-4:30



FACILITY ASSESSMENTS

Graeme Eastmure, Executive Vice President, Operations, Safeguard Security & Investigation Services Ltd.

The increasing number of Corporate Security Officers appearing high in corporate management structures shows the growing importance of facility security to a company's continued health. The assessment of a facility's safeguards and security can save not only revenue, but also lives, as facilities can be inspected to review preparedness for situations involving information security, workplace violence, weather and fire hazards. This workshop will provide you with best practices for assessing facilities and implementing improvements for 'safeguarding' your employees, clients and property.

- Conducting detailed reviews of your facility, including a security assessment
- Examination of physical and policy/procedural security issues including access control, CCTV, alarms and security guard requirements
- Facility risk assessment: targeting acts of terrorism, natural disasters, violent crime, work place violence, or activist assaults
- Points to consider during threat assessment and hazard identification
- Approach for considering human-caused incidents: terrorism, workplace violence, sabotage, and other malevolent behaviour
- Overall approach for performing a vulnerability assessment: how to prioritize vulnerabilities to identify greatest risk
- Facility security planning: key principles for a multi-hazard risk management program
- Evaluating facility protection options: considerations when evaluating countermeasures
- Carrying out a review of the architectural and environmental layout of facility
- Analyzing current security systems and practices
- Drafting list of security improvement and suggestions

Graeme Eastmure is founder and President of Safeguard Security & Investigation Services Ltd., where he oversees the handling of private investigation and security guard work for several corporations across the country. He has done extensive investigative work and specializes in pre-employment background checks for clients, undercover and sting operations, surveillance, interviewing suspects of theft, fraud and other criminal offenses. His successful work in making arrests for theft, fraud and illegal drug activity quickly led to a variety of investigative and management positions across Canada, during which time he became licensed as a private investigator in Ontario, Manitoba, Saskatchewan, Alberta and BC.

September 16, 17 & 18, 2009, Toronto

7th

Reinventing the Chief Security Officer

The Latest Innovations in Corporate Security Practices

"I found the real life stories from other companies very valuable. It wasn't just lots of theory, it was real people and real solutions."

"Well-rounded and well-balanced presentations - a good cross-section of security professionals - great learning environment."

"Good networking and contact building."

"Very thought provoking."

METROPOLITAN HOTEL, 108 CHESTNUT STREET, TORONTO, ONTARIO, M5G 1R3

TO REGISTER FOR CHIEF SECURITY OFFICER SUMMIT

Delegate Name _____
 Delegate Title _____
 Approving Manager Name _____
 Approving Manager Title _____
 Department _____
 Organization _____
 Address _____
 City _____ Province _____ Postal Code _____
 Telephone _____ Fax _____ e-mail _____

PAYMENT OPTIONS

Cheque enclosed (payable to Federated Press) for: \$ _____
 GST Registration # R101755163

Please bill my credit card: AMEX VISA Mastercard
 Credit Card # _____ Expiration date: ___/___/___
 Signature : _____

REGISTRATION COSTS

	Book & Pay by Jun 15/09	Book & Pay by Jul 13/09	Regular Price
<input type="checkbox"/> Conference + all workshops	\$2695	\$2795	\$2895
<input type="checkbox"/> Conference + 1 workshop (<input type="checkbox"/> A or <input type="checkbox"/> B)	\$2220	\$2320	\$2420
<input type="checkbox"/> Conference + CD-ROM (\$150)	\$1825	\$1925	\$2025
<input type="checkbox"/> Conference only	\$1675	\$1775	\$1875
<input type="checkbox"/> CD-ROM only			\$499

* Breakfasts, luncheons, morning and afternoon coffee breaks are included in the registration fees.
 Please add 5% GST to all prices. / PBN#101755163PG0001

CD-ROM: The modern way to benefit from leading-edge conference information. Weren't able to attend this Federated Press conference? Though you cannot replace the experience of attending, you can benefit from the leading-edge information provided at the conferences, including all the written materials and video presentations by purchasing the Proceeding CD ROM. Our conference CD-ROMs create the experience of actually being at a lecture or conference.

Mail completed form with payment to:

Federated Press
 P.O. Box 4005, Station "A"
 Toronto, Ontario
 M5W 2Z8

FederatedPress



1-800-363-0722
 Toronto:
 (416) 665-6868



info@federated
 press.com



(416) 665-7733

WHEN CALLING, PLEASE MENTION PRIORITY CODE: CSOT0909/E

Payment must be received prior to September 9, 2009

UNCONDITIONAL UPGRADE POLICY

If you have registered for a similar or simultaneous event and wish to attend this Federated Press event instead, we are so sure that you will find this conference of more value that we will refund any cancellation fee up to \$300.00

GROUP DISCOUNT

If you register four people at the same time you will be entitled to a discount. To take advantage of this special offer, payment for all delegates must be made with one cheque or credit card charge. Contact Sandra Frattolillo at: 1-800-363-0722 ext.223 for more information.

Cancellation: Please note that non-attendance at the conference does not entitle the registrant to a refund. In the event that a registrant becomes unable to attend following the deadline for cancellation, a substitute attendee may be delegated. A copy of the conference papers will be provided in any case. Please notify Federated Press of any changes as soon as possible. Federated Press assumes no liability for changes in program content or speakers. A full refund of the attendance fee will be provided upon cancellation in writing received prior to September 3, 2009. No refunds will be issued after this date.