January 25 & 26, 2011, Ottawa — Inaugural Two-Day Event!

Learn effective measures in breach detection and privacy protection

Preventing Data Breach & Misuse

Best practices for implementing and maintaining effective compliance

Workshop Included: Data Breaches: What To Do When They Happen?

participating organizations

AccessPrivacyHB
Anita Fineberg & Associates Inc.
Bell Canada
Canadian Institute for Health Information
Correctional Services Canada
Equifax Canada Inc.
Froese Forensic Partners
Lang Michener LLP
Nymity Inc.
Ontario Lottery & Gaming Corporation
PricewaterhouseCoopers LLP
Rogers Communications
Royal Canadian Mounted Police
Symcor Inc.

who should attend

CIOs, chief knowledge officers, and directors and managers involved in data protection, privacy, information management, knowledge management, IT, e-government, and information services

course highlights

- Hear from thoughts leaders and IM experts as they discuss best practices for data security and protection
- Look at best practices for protecting privacy when data is used in testing & training
- Examine best practices in fraud detection and prevention
- Examine the most common types of inside threats and best practices for protecting against them
- Examine the privacy risks associated with cloud computing
- Examine the issues involved in responding to a privacy breach
- Learn what the federal Privacy Commissioner's annual report has to say about the threats posed to data storage by the use of wireless wireless technology by goverment

Course Leader
Anita Fineberg, Anita Fineberg & Associates Inc.

Fariba Anderson, Ontario Lottery & Gaming Corporation

Michael E. Doucet, Royal Canadian Mounted Police

John Jager, Nymity Inc.

Mimi Lepage, Canadian Institute for Health Information

Kevin Lo, Froese Forensic Partners

John Russo, Equifax Canada Inc.

Howard Simkevitz, Bell Canada

Bobby Singh, Rogers Communications

Pamela Snively, AccessPrivacyHB

David M.W. Young, Lang Michener LLP

Della Shea, Symcor Inc.

Ted Reinhardt, Correctional Services Canaa

Derek Street, PricewaterhouseCoopers LLP

COURSE LEADER

ANITA FINEBERG
Anita Fineberg, LL.B., CIPP/C is the President of **Anita Fineberg & Associates Inc.**, a recently incorporated consulting company with a mandate to provide privacy solutions for the private sector, government and other public sector entities. She is both a lawyer and a CIPP/C (Certified Information Privacy Professional/Canada) who also maintains a legal practice specializing in privacy law.

CO-LECTURERS

FARIBA ANDERSON
Fariba Anderson is Vice President Lottery IT and Information Management at **OLG**. She is the single point of contact, senior advisor and spokesperson on information technology for Lottery and Bingo business lines.

MICHAEL E. DOUCET
As Chief Technology Officer for the **RCMP** , Michael Doucet is responsible for ensuring the CIO Sector has the technology necessary to maintain its services in support of **RCMP** strategic priorities.

JOHN JAGER
John Jager, CIPP/C, is an accredited and experienced privacy professional who has been **Nymity**'s Vice President of Research Programs for three years.

MIMI LEPAGE
Mimi Lepage is Chief Privacy Officer & General Counsel at the **Canadian Institute for Health Information**.

KEVIN LO
Kevin Lo, Managing Director at **Froese Forensic Partners Ltd.**, focuses his practice on electronic discovery and specializes in computer forensics.

JOHN RUSSO
John Russo is Vice President, Legal Counsel for **Equifax Canada Inc.** His responsibilities include global sourcing, all security and compliance, government and legislative relations, corporate governance and privacy functions.

DELLA SHEA
Della Shea is the Chief Privacy and Information Risk Officer at **Symcor Inc.**, which recently received the HP-IAPP Privacy Innovation Award for 2010.

HOWARD SIMKEVITZ
Howard Simkevitz is a Senior Associate Director at **Bell Canada** where he provides privacy consulting services. He also serves as a trusted advisor to the Bell Privacy Centre of Excellence.

BOBBY SINGH
Bobby Singh has 16 plus years experience in information security with extensive experience in risk management, business operations, public relations, consulting and auditing. As the Director of Information Security and Risk Management for **Rogers Communications** (RCI), his role involves ensuring that security is built-in both at the organization-level and within RCI products and services.

PAMELA SNIVELY
Pamela Snively is a lawyer with **AccessPrivacyHB**. She provides a broad range of privacy, risk management and compliance advice in the private, public and health sectors.

DAVID M.W. YOUNG
David M.W. Young is a Partner and co-chair of the Privacy Law Group at **Lang Michener LLP**. His practice focuses on regulatory law. Mr. Young is recognized in The Canadian Legal Lexpert Directory 2010, as a leading practitioner.

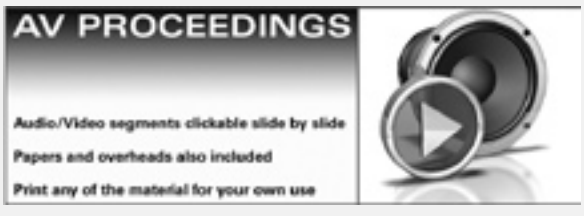
TED REINHARDT
Ted Reinhardt is Director of IT Security and Project Management at **Correctional Services Canada**.

DEREK STREET
Derek Street is Senior IT Security Architect at **PricewaterhouseCoopers LLP**'s Ottawa office.

SUPPLEMENTARY COURSE MATERIAL

Federated Press is now providing delegates with access to an innovative new database containing at least 25 interactive multimedia presentations by leading experts and approximately 20 hours of lectures on the topics covered by this course, including all slides and speakers' papers. See the list of presentations on page 4.

Delegates will also receive a trial subscription to the Technology Channel, a much broader resource representing hundreds of hours of interactive multimedia lectures on leading edge technology topics as delivered at our many recent technology conferences and courses.



NEW TECHNOLOGIES IN DATA PROTECTION

As the number and the sophistication of threats to data security increases, so too have the number and variety of information security technologies. This session will examine the major developments in new authentication techniques and privacy technologies in data protection as well as forecast the next generation of security controls.

- Breakthrough approaches to pre-emptive security and "self-healing" computing solutions
- Data-level security and privacy controls: latest authentication tech niques
- Latest developments in security information management systems
- Intrusion Prevention and Protection Systems (IPS)
- Multi-level malware protection systems
- Use of identification & authentication controls
- Developments in the protection of the mobile storage devices

PRIVACY CONCERNS WITH CLOUD COMPUTING

Many organizations are turning to cloud computing as a means of increasing efficiency and saving on operational costs in their IT services, as it is seen as a cheap, viable option for data storage and processing. While the benefits of the cloud are many, it is important for organizations to recognize the risks associated with this type of solution. This presentation examines the data security risks associated with cloud computing and suggests a strategy for mitigating such risks by focussing on legislative requirements and adherence to industry best practices.

- Data security challenges and risks associated with cloud computing: data access; infrastructures and accountability; data integrity attacks
- Promoting practices that protect personal data
- Investing in a framework for managing data security in the cloud

PROTECTING PERSONAL DATA FROM INSIDE THREATS

While it is most common to think of data security breaches in terms of hackers taking advantage of vulnerable network or infrastructure security or poor server or database security standards, the largest threat of a data breach comes from inside your organization, from disgruntled employees. This session examines the most common types of inside threats and best practices for protecting against them.

- Protecting the information held by employees
- Managing and securing the access of employees
- Security risks of the growing forms of media used by employees
- Establishing whistle blowing practices
- Conducting workplace investigations
- Overcoming digital identity management infrastructure challenges
- Integrating digital credentials: PKI certificates, etc.

PROCTECTING PRIVACY WHEN DATA IS USED IN TESTING & TRAINING

Data security practices for protecting privacy and reducing the risk of data breaches for production environments are not always effective when applied to data in non-production environments, where developers, testers and trainers require access to realistic data. As such, testing and training environments can pose and extra threat to an organization. This session will look at best practices forprotecting data that is used in testing & training.

- What are organizations really using for test data?
- How to manage the test data issue with your outsourcers
- Hear the results of a recent North American benchmarking study
- How have the PCI standards changed the game?
- Mitigate privacy risks when they must use production data in testing
- Are de-identification and masking the panacea?
- Application-aware masking capabilities
- Prepackaged data masking routines to de-identify data

DETECTING DATA BREACHES

Protecting against data breaches is an increasingly difficult task, as they can result from a wide range of actions from a growing list of player. These breaches may occur as a result of inadvertent errors or malicious actions taken by employees, third parties, partners in information-sharing agreements or hackers. This session will examine the most effective measures in breach detection.

- Advanced techniques and best practices for data breach detection
- How data breach detection fulfills compliance requirements
- Measures to detect data breaches in outsourced agreements
- Real time alerts: automated intrusion detection and analysis technologies
- Outlining the required procedures for response and recovery of information
- Incident handling procedures

BRIDGING THE GAP BETWEEN DATA PROTECTION & IT

Efficient, effective, and innovative information technology is key to achieving well-managed and protected information. In order to establish a secure data environment and minimize the threat of security breaches, it is crucial that there exists a close working relationship between the Data Protection professionals in your organization and your IT department. This session will examine how these two areas of your organization must work together to in order to fully protect your data.

- Overview of IT security principles and governance issues
- Working together to uncover infrastructure weaknesses to protect against malicious attacks and cyber crime
- Understanding the needs and constraints of both departments
- Improving data management to address concerns of the IT department
- Common areas of concern: risk assessment, awareness, cyber threats, privacy vs transparency, information integrity

PREVENTING & DETECTING IDENTITY THEFT

Every year, thousands of people are victims of identity theft. Whether it is as a result of employee wrongdoing in the workplace or as a result of outside criminals laying their hands on personal information, it is one of the most prevalent types of fraud. This presentation will examine how identity theft occurs and discuss prevention measures.

- Identifying traditional and new type of fraud schemes and scenarios: fraud risk assessments
- Defining the types of identity theft and how it can occur
- Prevention measures: physical security, data security, data checks
- Phishing, workplace identity theft, access cards
- Dealing with identity theft through use of government issued documents
- Promoting greater awareness of the possible risks among your employees

INFORMATION AND DATA SHARING/INTEROPERABILITY

In today's environment, the need for data sharing in the public sector continues to increase at a rapid pace. However, this sharing of personal information must not unreasonably infringe on privacy rights. All sharing of personal data must therefore comply with data protection laws and effectively deal with the inherent risks. This session examines the challenges associated with information sharing and the practical issues and challenges in dealing with the risk to privacy.

- Legislative developments affecting information sharing in the public sector
- Best practices for sharing data within and across organizations
- Identifying the risks associated with data sharing: ensuring privacy and security risks are understood, addressed and managed
- Best practice in data protection between public and private sector organizations
- The role of Privacy Impact Assessments
- Trans-border considerations in information sharing

DATA SECURITY & COMPLIANCE: EFFECTIVE MEASURES

All Canadian organizations in both the public and private sectors are legally responsible for ensuring that their personal information holdings are secured against unauthorized access, disclosure or other events that may give rise to potential data breaches. This session will examine effective measures that can be taken by your organization in order to comply with data security requirementsand provide best practices for implementing and maintaining effective compliance procedures.

- The legal framework: Canadian privacy legislation and regulations, government policies and industry best practices
- Ensuring that administrative, physical and technological safeguards and controls have been implemented and are maintained
- Meeting compliance requirements and managing risk with data breach detection
- Ensuring that sharing of personal information complies with applicable laws
- Effective measures for the preservation and archiving of electronic documents
- Protecting local WiFi networks with the recommended encryption guidelines

THE FUTURE OF TECHNOLOGY-RELATED CRIME

IT and IM professionals frequently react to data breaches that have occurred, but what are the types of technology-related crimes that the future holds? This presentation will explore what you should watch out for.

- The future of technology-related crime
- What to watch for
- Common areas of concern
- Promoting greater awareness of the potential risks among IT and IM professionals

WORKSHOP

DATA BREACHES: WHAT TO DO WHEN THEY HAPPEN?

Regardless of all steps taken to protect your data, it is impossible to totally eliminate the risk of a data breach. This is why organizations should be required to establish a plan for addressing data breaches that sets out roles and responsibilities, lists internal procedures and communications requirements, and provides for notification standards and procedures, including the timing of such notification. This interactive workshop will examine the issues involved in responding to a data security breach.

- Establishing a plan setting out what to do in the event of a data breach
- Taking immediate action to stop the breach and to secure affected data
- Documenting the breach
- Identifying the individuals affected by the breach
- Notifying the appropriate bodies and individuals whose personal information has been wrongfully disclosed, stolen or lost
- Conducting an internal investigation
- Making recommendations to prevent recurrence

Registration: To reserve your place, call Federated Press toll-free at 1-800-363-0722. In Toronto, call (416) 665-6868 or fax to (416) 665-7733. Then mail your payment along with the registration form. Places are limited. Your reservation will be confirmed before the course.

Location: Novotel Ottawa , 33 Nicholas Street, Ottawa, Ontario, K1N 9M7

Conditions: Registration covers attendance for one person, the supplementary course material as described in this document, lunch on both days, morning coffee on both days and refreshments during all breaks. The proceedings of the course will be captured on audio or video. Multimedia proceedings with all slides and handouts can be purchased separately on a CD-ROM which will also include the course material.

Time: This course is a two-day event. Registration begins at 8:00 a.m. The morning sessions start promptly at 9:00. The second day ends at 4:00 p.m.

Cancellation: Please note that non-attendance at the course 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. 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 January 12, 2011. No refunds will be issued after this date. Please note that a 15% service charge will be held in case of a cancellation.

Discounts: Federated Press has special team discounts. Groups of 3 or more from the same organization receive 15%. For larger groups please call.

Payment must be received prior to January 18, 2011

Phone: 1-800-363-0722 **Toronto: (416) 665-6868** **Fax: (416) 665-7733**

TO REGISTER FOR DATA PROTECTION

Name _____

Title _____ Department _____

Approving Manager Name _____

Approving Manager Title _____

Organization _____

Address _____

City _____ Province _____ Postal Code _____

Telephone _____ Fax _____ e-mail _____

Please bill my credit card: ❒AMEX ❒VISA ❒Mastercard

_____ Expiration date: ____ / ____

Signature : _____

Payment enclosed: ❒ Please invoice. PO Number: _____

WHEN CALLING, PLEASE MENTION PRIORITY CODE:

1DP1101/E

MAIL COMPLETED FORM WITH PAYMENT TO:
Federated Press P.O. Box 4005, Station "A"
Toronto, Ontario M5W 2Z8

REGISTRATION COSTS

NUMBER OF PARTICIPANTS: ____

COURSE: $1975

COURSE + PROCEEDINGS CD-ROM:
$1975 + $175 = $2150

PROCEEDINGS CD-ROM: $599

NOTE: Please add 13% HST to all prices.

Proceedings CD-ROM will be available 60 days after the course takes place

Enclose your cheque payable to Federated Press in the amount of:

GST Reg.# R101755163
PBN#101755163PG0001

For additional delegates please duplicate this form and follow the normal registration process