



## The Many Facets of Practical Information Protection SESSION DESCRIPTIONS

---

### **Keynote: The Debut of New Information Destruction Best Practices Guidelines**

***Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario***

In response to the continuing occurrence of improper, unsecure disposal of personal information, Dr. Ann Cavoukian, Ontario's outspoken and world renowned Information and Privacy Commissioner, worked with thought leaders in information security and records management to help her create concise and easy to apply information disposal principles to help organizations fulfill their legal information protection responsibilities. In this session, Dr. Cavoukian will unveil the new Information Destruction Best Practice Guidelines and explain how this often neglected area of information security can be easily brought into legal compliance.

### **Data Breach Notification Requirements: Common Denominators**

***Joanne McNabb, Chief California Office of Privacy Protection***

Like Ontario, California has been a leader in advancing stronger information protection principles. California was the first jurisdiction in the world to mandate that organizations notify authorities and affected individuals in the event their data has been breached. Since then, Data Breach Notification has swept the world, becoming one of the most effective and feared data protection compliance tools. And, while Data Breach Notification in some form is now present to some degree in Canada, privacy experts believe it is only a matter of time before legislation creates a strong Data Breach Notification requirement in Canada and around the world. In this session, Joanne McNabb, Chief of the California Office of Privacy Protection, will explain what a strong notification provision will look like and the impact of compliance on affected organizations.

### **End to End Encryption: The Keys to the Kingdom or an Open Back Door**

***Nandini Jolly, President and CEO, Cryptomill Technologies, Ltd.***

***James Young, Senior Manager, Global Information Security, PricewaterhouseCoopers***

Headlines like "Stolen Laptop put Thousands at Risk" and "Computer Tape Lost in Transit" seem to be weekly occurrences. When it happens, the first thing everybody asks is "Was the data encrypted?" Encryption is increasingly seen as a major component of any information security program. It is often represented as making the difference between an embarrassing and costly breach notification catastrophe and a "slight inconvenience". On the other hand, a noted encryption thought leader recently said "Anyone who thinks that encryption is the answer to their data security problems doesn't understand encryption or their data security problems."

This session will explain a wide variety of practical ways to apply encryption technology to stored information as well as information in transit. Attendees will also leave with a well rounded perspective on the ability of encryption to meet their information security needs.

### **New Rules, Part 1: Due Diligence in Vetting Data Related Contractors**

***Jeff Green, Chief Privacy Officer, Royal Bank of Canada***

***Derek Knights, Senior IT Security Governance Specialist, Sun Life Financial***

One of the growing realities of data protection is the inevitability of sharing sensitive information with service providers. For better or worse, organizations have a responsibility to select and manage these data management partners. In fact, these data management partners are often the weakest link in an information protection program. In this session, representatives charged with developing and managing such relationships at some of Canada's most respected corporations will discuss how to make sure your internal protections are not negated by negligent or unqualified contractors.

### **New Rules, Part 1: Due Diligence in Vetting Data Related Contractors**

***Jeff Green, Chief Privacy Officer, Royal Bank of Canada***

***Derek Knights, Senior IT Security Governance Specialist, Sun Life Financial***

Let's face it, you can't look over the shoulder of every employee making sure they comply with established information security procedures. On the other hand, without that compliance, those same employees render the best information protection policy useless. In this session, our panel of expert practitioners will turn their discussion to how to promote employee ownership in this critical area. Among the issues explored are in-house monitoring programs, the most effective training strategies, and how and when disciplinary actions come into play.

### **The Fast Track to No-Nonsense Policies and Procedures**

***Robert Johnson, Executive Director, NAID***

There was a day when an information protection policy could read "Protect Sensitive Information from Unauthorized Access." While those days are long gone, there is as much art as there is science in crafting legally required written information protection policies to thread the documentation needle. Too little direction and your organization runs the risk of non-compliance; too much and employees are set up for failure, resulting in non-compliance issues in that regard. In this session, a 30-year veteran of the information protection industry will discuss how to effectively meet the requirements to provide adequate direction to employees while not hemming them into compliance processes that will cause more trouble than they are worth.