



Office of the Chief Information  
and Privacy Officer

# Protecting Personal Information: *Managing Threats from Within*

**Mark Vale, Chief Information and Privacy Officer**  
**Government of Ontario**  
**PIPA 2008**  
**Calgary, Alberta**  
**November 17, 2008**



# Some Assumptions

- Risk probability can never be reduced to 0%
- Need to plan adequately, provide clear direction and support to all employees, and monitor
- Contractors and third-party providers are part of our business
- Need to be able to distinguish between errors of omission and errors of commission
- Effective mitigation will come when organizational norms and values – the culture – shape expectations and behaviour of employees
- Tested incident response plans are essential

# Overview

## Planning

- Risk Assessment
- Incident Response Plan
- Communication Plan

## Directing

- Standards & Practices
- Building Awareness
- Training
- Support Tools
- Roles & Responsibilities
- Accountability Regime

## Controlling

- Refresh Cycle on Direction
- Automated Process Controls
- Integrate with other Control Processes -- Program and System Development

## Evaluating

- Types of Evaluation
- Reporting Procedures
- Evaluation to Inform Action

# Planning

- **Risk Assessment**
  - Assessment to include:
    - Sensitivity of information
    - Who is involved (employee, contractor, external service provider)
    - Information process (collection, storage, transmission, disposition)
    - Where (on-site, teleworkers, mobile workers, 3<sup>rd</sup> party providers)
    - Integration of physical and electronic risks
    - Likelihood/Probability and Impact
  - Output: Risk rating and mitigation strategies
- **Incident Response Plan**
  - Procedures and Clear Roles and Responsibilities
  - Escalation to Senior Decision-Makers
  - Lessons Learned
- **Communications Plan**
  - High-level communication of program and who to contact
  - Identification of subordinate communications plans for specific audiences and contexts

# Directing

- **Standards and Practices**
  - ❑ Classification of information
  - ❑ Storage, transmission, and destruction of personal information
  - ❑ Acceptable access and use
  - ❑ Contracting with 3<sup>rd</sup> parties
  - ❑ Telework and mobile work practices
- **Building Awareness**
  - ❑ Information campaigns for different audiences and contexts
  - ❑ Sustaining messaging and positive tone
- **Training & Support Tools**
  - ❑ Multi-modal
  - ❑ Context specific (working at home; working in a hotel)
  - ❑ Automated support tools (e.g. encryption of laptops)
  - ❑ Model practices (e.g., sample contract clauses)
- **Roles and Responsibilities/Accountability**
  - ❑ All levels of the organization
  - ❑ Clear communication of consequences

# Controlling

- **Initial Action and Refresh Cycle for Each Direction Activity**
  - ❑ Employee orientation, sign-up for telework, RFP and contract negotiation
  - ❑ Annual performance reviews and re-declaration of employee understanding
  - ❑ How to sustained awareness campaigns
  - ❑ When to update training programs and materials
  
- **Automated Process Controls**
  - ❑ Access controls (physical and electronic)
  - ❑ Automatic encryption of laptops
  - ❑ Authorized portable storage devices
  - ❑ Disposition of electronic devices, including end of lease provisions
  
- **Integrate with Other Process Controls**
  - ❑ Project gating
  - ❑ Budget approval
  - ❑ Entry/exit protocols

# Evaluating

## ▪ Types of Evaluation and Purpose

- ❑ Benchmarking (maturity assessment)
- ❑ Program Review (effectiveness)
- ❑ Management Audit (compliance)
- ❑ Forensic Audit (investigation and enforcement)

## ▪ Reporting Procedures

- ❑ Who receives formal report of evaluation
- ❑ Broader communication strategy (can support improvement)
- ❑ Appropriate frequency of evaluation

## ▪ Informed Action

- ❑ Changes to program and support materials
- ❑ Corrective action – changes in processes and practices
- ❑ Contract management
- ❑ Human resources management

# Final Thoughts

- Generally we are at a fairly low state of maturity in this area – somewhere between *ad hoc* and defined – or 1.5 out of 5
- We are building organizational values and norms, but must mitigate real risk as we do it
- Don't forget reward and recognition programs
- Be up front with employees about expectations, monitoring practices and consequences
- The organization's boundaries include contractors and 3<sup>rd</sup> parties
- Follow through on what we say
- We must be vigilant....and practical!

**Mark Vale, Ph.D.**  
**Chief Information and Privacy Officer**  
**Government of Ontario**  
**Ministry of Government Services**  
**77 Wellesley St. W, 5<sup>th</sup> Floor Ferguson Block**  
**Toronto, ON M7A 1N3**

**Tel: 416.327.1450**

**Email: [mark.vale@ontario.ca](mailto:mark.vale@ontario.ca)**