Getting Accountability Right with a Privacy Management Program

PIPA 2013

Vancouver

About David Hughes:

- former Director of Privacy for BCLC:
  - “His work on establishing a significant Privacy regime in BCLC was critically important to the organization and he was successful in ensuring Privacy became a part of our fabric.” – Michael Graydon, President and CEO
- co-teaching Information and Privacy Law at Thompson Rivers University, with David Loukidelis Q.C.
- Partner at Forward Law LLP

About Barb Bucknell

- Senior policy advisor with Office of the Privacy Commissioner of Canada
- Investigator, special advisor, OECD and Treasury Board Secretariat.

About Drew McArthur

- Principal of the McArthur Consulting Group
- Former Compliance Officer at TELUS
- Member of Liz Denham's External Advisory Board

Agenda

- Accountability – an overview
- Scenario for the workshop
- First steps to accountability
  - Executive buy-in and ownership
  - Senior team commitment
- Tools for accountability
  - Privacy Impact Assessments
  - Privacy risk identification
  - Risk management surveys and control functions
  - Employee programs and focus
- What you can do

Accountability

- Acceptance of responsibility for personal information protection
- The first among the fair information principles (in PIPEDA)
  - Policies, procedures that promote good practices
  - Taken as a whole = privacy management program

Privacy Management Program

- Goal – compliance with applicable laws

- Effects – trust and confidence
- Effects – enhanced competitiveness, reputation

Building blocks

- Organizational commitment – internal governance structure
  - Buy-in from the top
  - Privacy officer
  - Privacy office (depending on size of org)
  - Reporting

Building blocks

- Program controls (continued)
  - Training and education requirements
  - Breach and incident management response protocols
  - Service provider management
  - External communication – public-facing policies

Ongoing Assessment and Revision

- Develop and Oversight and Review Plan
- Assess and Revise Program Controls
- Demonstrable

Tales from the front

- Good news – some organizations take accountability very seriously
  - Thorough, up to date data mapping
  - Training implemented after problems brought to light
- Bad news –

Tales from the front

- …and the bad news – still some fundamental problems:
  - no privacy officer in place
  - wrong contact info
  - lack of recognition that the “problem” is a privacy one

Tales from the front

- Accountability-related issues appear to be on the rise

Unhappy customers? Unhappy complainants.

Executive Buy-in

- Where's your company with respect to recognizing Privacy as one of the key pillars of compliance?
- Can you write a supporting letter from the CEO?
- Meet with the senior team members to explain the program
- Engage as many as possible in the initial meetings to raise awareness
- Have an executive or senior manager own each of the key databases in your company

sell it to the executive

- introduce them to the change (then/now)
- suggest to them why it matters to their business
- show them the potential costs
- show them the dirt
- show them the dream
- make your ask

then / now

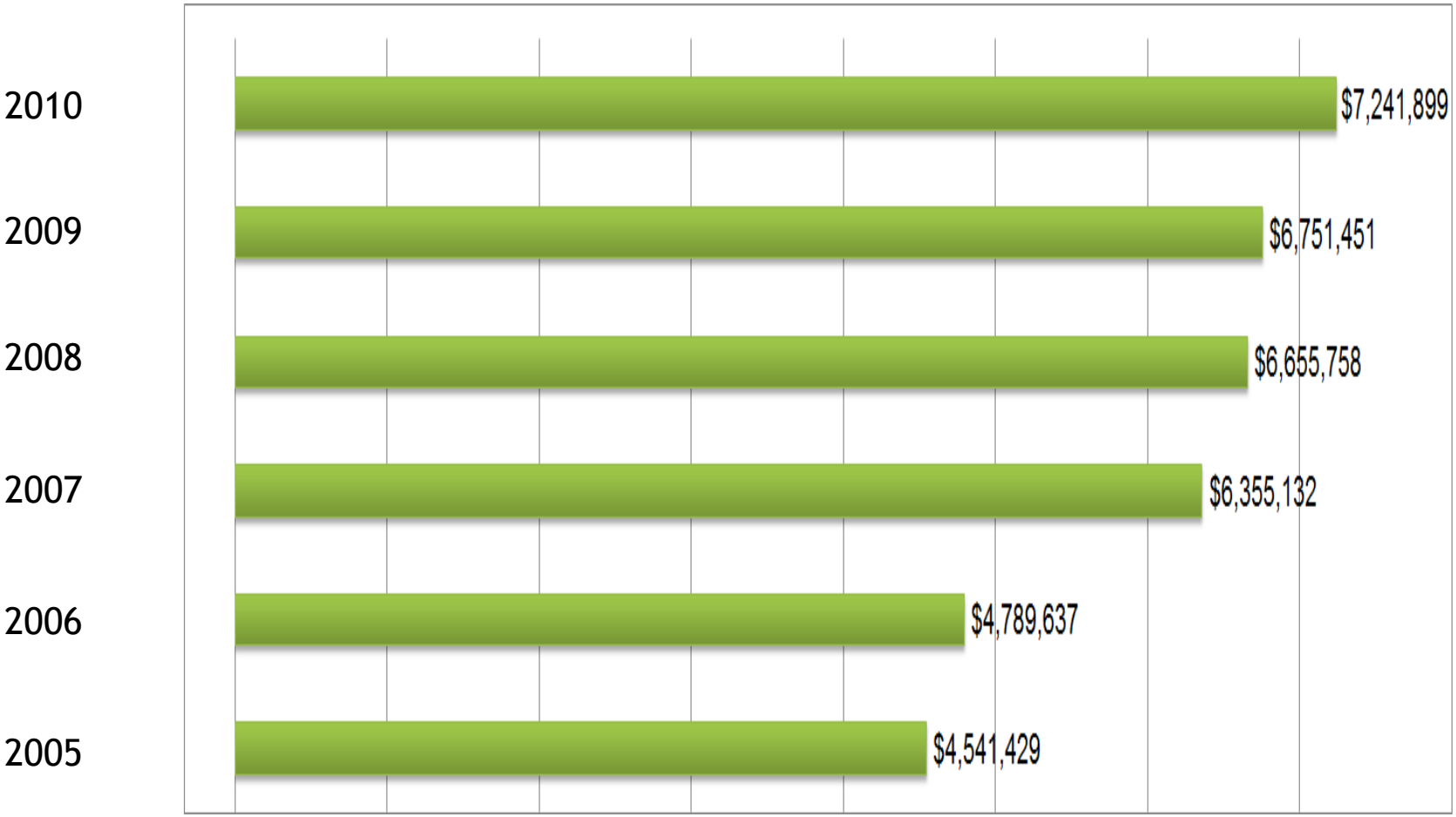
- then:
  - privacy = being out of sight
    - having a policy
    - making sure in compliance with external requirements (law)
- now:
  - privacy = being in control of personal information
    - managing personal information throughout its lifecycle

why does it matter?

- for revenue growth – “the lifeblood of the digital economy”
- the risks posed by privacy breaches are huge
- because we have a dedicated watchdog
- it matters to our customers

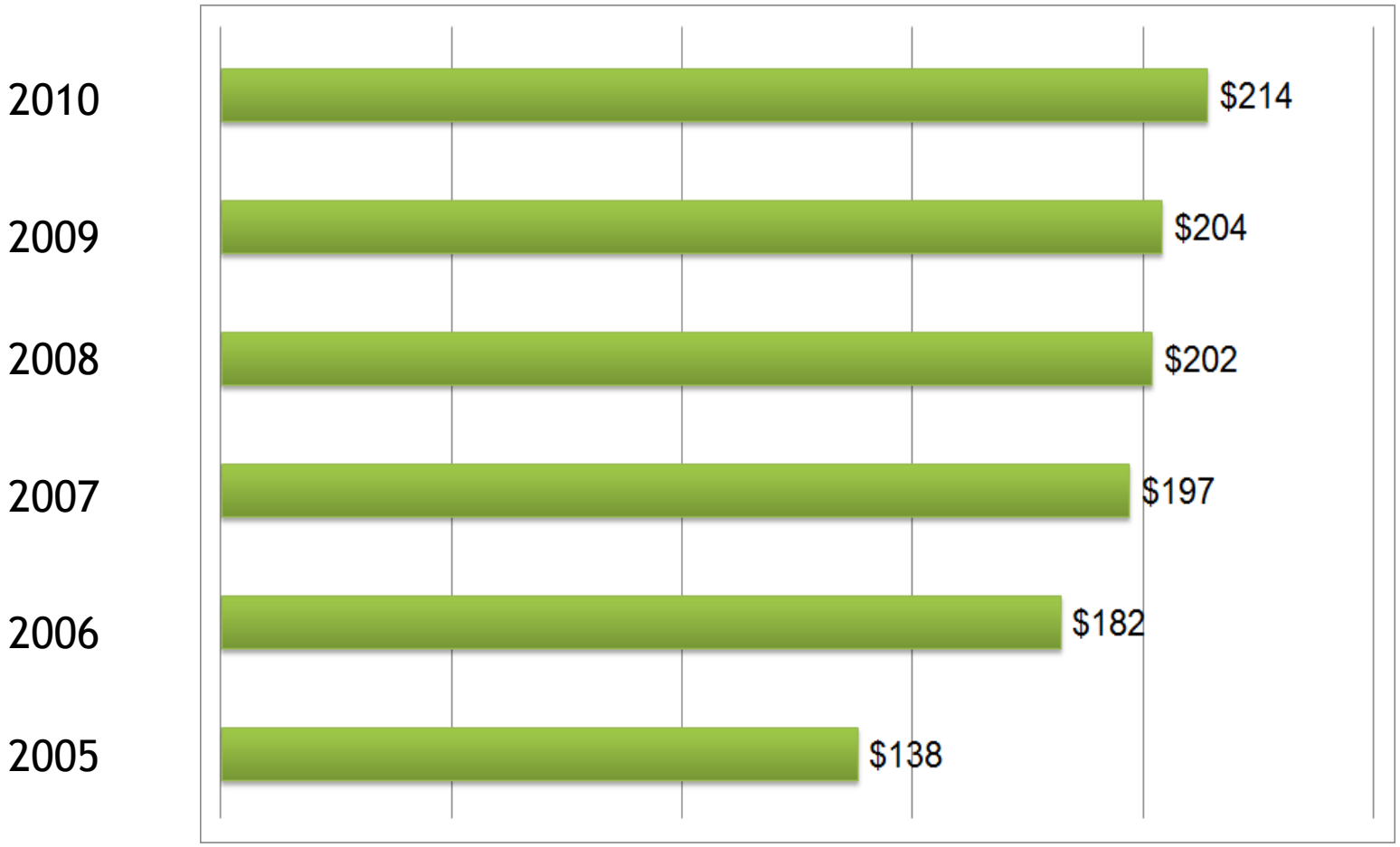
Cost of Data Breach. Sponsored by PGP Corporation. Presented by Dr. Larry Ponemon. *Ponemon Institute* LLC

Average Organizational Cost of a Data Breach



Average Per Record Cost of a Data Breach

Cost of Data Breach. Sponsored by PGP Corporation. Presented by Dr. Larry Ponemon. *Ponemon Institute* LLC



the dirt

- the emails from customers
- the emails from internal staff
- the bullets dodged

the dream

“we can tell you:

- all the places where we store your personal information;
- all the people who have access to it;
- how it is secured and how long we retain it;
- all of our employees and service providers who touch your information have completed and passed privacy training; and
- all of our vendors adhere to industry-leading compliance requirements if they want to do business with us.

“what matters to you matters to us.”

the ask

- executive communications (buy-in from top)
- corporate-wide PIA policy (policies)
- corporate-wide project (inventory, policies and training)

Motivating Scenario

(Provided courtesy of the Office of the Privacy Commissioner of Canada)

- You are a privacy professional, and have just received a call from the CEO of a private sector Canadian organization. She tells you that the organization hasn't examined their privacy practices in some time and are concerned about potential exposures. They would like you to help them get accountable!

You are given the following information

(Provided courtesy of the Office of the Privacy Commissioner of Canada)

About the business	Volume and sources of personal information
Sector: Retail Age of business: 5 years Number of executive: 7 at ‘Director’ level or higher Number of employees: 800 Jurisdiction: Offers services in multiple provinces	Loyalty program (used for behavioural targeting, discounts, targeted mailouts and emails •Approx 10K customers registered •20K-50K transactions recorded per month •Customer profile contains name, age, gender, email address (optional), transaction history, inferred consumer segment (income, preferred products, etc)

More sources of personal information:

- “Refer a friend” program
  - Submit your name and contact information, and that of a friend, to be entered into a monthly draw
    - ~2K submissions per month
- Records kept of name and driver's license number for all returns
- Video surveillance in use in most locations

(Provided courtesy of the Office of the Privacy Commissioner of Canada)

Key considerations	Other factors
• Strong buy-in from the top (now) • Few formal privacy structures in place • CPO an unofficial role, filled by lowest ranking executive • 20% annual employee turnover • New employee training focuses on product knowledge, not policy	• CEO loves innovation, and is considering in-store WiFi, a mobile app, mobile payments, predictive analytics, etc. • Organization has significant expansion plans, possibly internationally

(Provided courtesy of the Office of the Privacy Commissioner of Canada)

Workshop Exercise #1

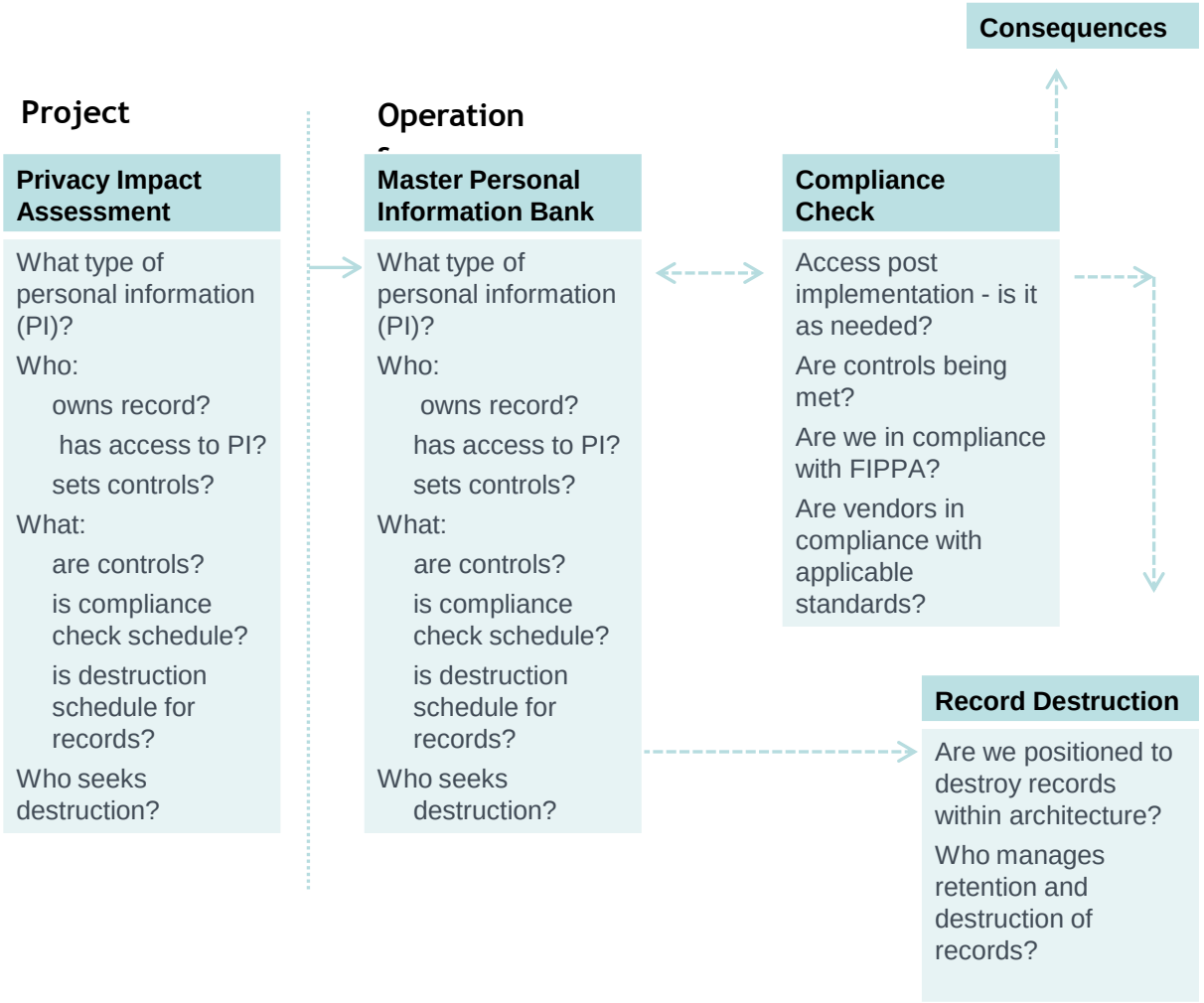
Answer the following questions:

1. How can the newly minted privacy manager generate executive buy-in at the company in the scenario?
2. What are some specific steps they can take to actually get commitment?
3. What kind of commitment are you looking for?

Accountability tools that work

- Privacy Impact Assessments
  - When do you need one?
- PIA questionnaire
  - Long Form PIA
  - System PIA
  - PIA amendment
  - Privacy standard
  - Privacy advice

beyond PIAs: complete lifecycle management



potential project deliverables

- inventory of all personal information in organization's custody or control
- improved framework for governance of personal information at organization
  - who, what, when, why; and
- tool for consistent tracking and management of personal information

one way to structure an inventory

- core identifiers
  - first name, last name, SIN, credit card number etc.
- secondary information
  - (linking information) – loyalty card number, financial transactions, web history, social media
  - links to outside databases or applications
- collection and stewardship
  - purpose of collection, how consent was obtained, current use
  - business, IT and secondary stewards of information
- security
  - current security controls around that information

Workshop Exercise #2

What questions do we need on a PIA to meet the needs of the organization in our scenario?

The Employee Factor

- Do your employees know about privacy?
- Do they know who the privacy officer is?
- If you have a privacy office, do they know about you?
- Do they know how to recognize a “privacy” issue?
- Do they know how/where to escalate?

Accountability tools that work

Training Programs

- Ideally these are annual
- Depending upon the type of organization and complexity of the information flows
- On-line training with use of examples
- Include security training with privacy training – two birds with one program!
- Regular prompts and communications can keep training alive
- New situations should be pushed out quickly and easily to employees

The Employee Factor

- Don’t forget about your employees’ privacy

Workshop Exercise #3

1. What are some elements of an effective employee training program for the company in our scenario?
2. What steps can be taken to reinforce the training and keep it relevant?

Tips

- Have correct contact information for privacy on your website
- Have lunch with as many people you can in your organization
- Executive ownership
- Review, refresh and revise regularly

make governance everyone's job

- classify processes by risk
- identify owners of processes / data / security
- identify catchpoint for new processes / data / vendors
- update role profiles
- appoint privacy auditors
- schedule checks (red/yellow/green)
- tie in with Calendar
- have standardized consequences communicated in advance

David Hughes
dhughes@forwardlaw.ca
1 (855) 434-2333
@davidfwd

Forward Law LLP
203-1211 Summit Drive
Kamloops, BC
V2C 5R9

Questions?

- Joint Guidance document available at: http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp
- Contact information:

drew.mcarthur@telus.net

604 220-2105

Barbara.bucknell@priv.gc.ca

613 943-5549