



Diagnosing and fixing privacy breaches

Drew McArthur
Member of the TELUS Team

2007 PIPA Conference, Vancouver B.C.



Here's my agenda

- A plug for breach guidelines
- Business continuity planning
- Case study
- Who you going to call?



Breach Notification Guidelines

- Collaboration of industry groups across Canada with Privacy Commissioners
- Voluntary guidelines for industry on how to manage a data breach
- Posted by New Zealand Privacy Commissioner as basis for public comment
- http://privcom.gc.ca/media/nr-c/2007/nr-c_070801_guidelines_e.pdf



Business Continuity Planning

- Step one: make sure you have a plan
 - Use the breach notification guidelines as an outline, then customize it to your organization
- Step two: make sure people know about the plan
- Step three: make sure you refer to the plan
 - Ensure organization follows the plan
- Most important step is to learn from the event
 - Remember, hard lessons are difficult to learn, so be gentle but firm with your colleagues



Case Study

- What goes on the road stays on the road? Agreed?
- Diagnosing a breach is not necessarily an easy exercise
 - Remember the server hard-drive that fell into the hands of a student?
- You may need a phased approach to a breach
- What would you do in the following circumstances?



Who you going to call?

Call now, operators are standing by

- Call your friendly neighbourhood privacy commissioner
 - It might be a good idea to give them a “heads up”
- BUT: (there’s always a BUT) make sure you discuss what your neighbourhood commissioner is going to do with the information
- Call the customer?
- Others?
- Over to you Frank Work

