

Responding to Data Breaches



Agenda



- Introduction
- How to Respond to a Breach
- 5 Things You'll Wish You Had Done



Thieves steal Vancouver client
information from TD bank

Massive Security Breach
Could Affect Homeowners
Thousands Of Vermonters At Risk

**Best Western forced to play
defense on data breach disclosure**


Could hotel chain have done a better job of defusing
story about system intrusion?





How to Respond to a Privacy Breach

Four Key Steps:

1. Contain
 2. Evaluate
 3. Notify
 4. Prevent
- 

Step 1: Contain the Breach

- Activate your breach management policy
- Take immediate, common sense steps to limit the breach



Activate Your Breach Management Policy

- Get Organized
- Get the Facts



Common sense containment

- Retrieve the lost or stolen information
- Address weaknesses in physical security
- Address weaknesses in technical security



Step 2: Evaluate the Risks

- Nature and sensitivity of the personal information
- Individuals affected
- Cause and extent of the breach
- Foreseeable harm



Step 3: Notification

- Who
- When
- How
- What



Step 4: Prevention

- Improved physical security
- Enhanced security architecture
- Policies
- Training
- Contractor supervision
- Audit schedules



5 Things You'll Wish You Had Done

1. **Audit**
2. **Assume a breach will happen**
3. **Limit your collection of personal information**



5 Things You'll Wish You Had Done

4. Encrypt

5. Create a privacy conscious culture

