

DATA BREACH RESPONSE - A Multidisciplinary Perspective

Dan Michaluk of Hicks Morley
djm@hicksmorley.com
<http://danmichaluk.wordpress.com>
(416) 864-7253

David Malamed of Grant Thornton LLP
dmalamed@GrantThornton.ca
(416) 360 -3382

Agenda

- Current state
- Data breach in the news
- Legal risk
- The forensic investigation
- Reputation risk
- Crises management
- Prevention

Current State of Affairs

- Do your clients have breach response plans?
- What often happens?
 - Finger pointing and uncertainty
- Breach response planning – why
 - This is an “action challenge”
 - Command and control model works
 - Before better than after
- Breach response planning – what
 - What risk-based assessments will be made?
 - By whom?
 - Based on what information?

Effects

- Hard costs
- Customer loyalty
- Investor relations and finance difficulties
- Regulatory scrutiny
- Civil claims (through class action!)
- Contractual damages

News Article Synopsis #1

- TJX/Winners Breach
 - Multiple breaches - 2003 to 2006
 - 46 million customer
 - Payment cards (large unascertainable set)
 - DL and ID numbers (small set)
 - Two-phase notification
 - Class action recently settled
 - Canadian privacy investigation

News Article Synopsis #2

- Talvest Mutual Funds
 - Hard drive lost (470,000 mutual fund customers)
 - Names, addresses, signatures, dates of birth, account numbers, beneficiary information and social insurance numbers
 - Promise to compensate for “direct monetary loss” and pay for credit monitoring
 - Privacy Commissioner investigating anyway

In The Event of A Breach...

- A forensic investigation
- An evaluation of contractual obligations
- An evaluation of exposure to liability
- Risk management and crises control

Key Legal Risks

- Risk 1: Breach of duty to secure
 - For the current breach, need to understand the potential defence
 - Negligence depends on cause of loss
 - Causation depends on what was lost
 - For the next breach, need a documented root-cause analysis and remedial plan

Key Legal Risks

- Risk 2 - Breach of duty to warn of reasonably foreseeable harm
 - Information informs both the notification strategy and the mitigation strategy
 - This is time sensitive – “at the first reasonable opportunity”

Forensic Investigation

- Key questions
 - Why did it happen? (malicious or benign)
 - How did it happen?
 - Who was affected?
 - What data was lost?
 - Can effected people be grouped?
 - Can it be remedied?

Forensic Investigation

- Precise Information
 - Ability to report the facts
 - Fact gathering
 - Interviews
 - Data Extraction
 - Database Building
 - Breach Reconstruction
- How much time do you have to complete the investigation?

Reputation Risk

- The media will take an interest
 - Identity theft is interesting to people
 - Does it outweigh financial risk?
 - Solution:
 - » Quick response
 - » Knowledge
 - » Communication Planning

Crisis Management

- Is notice given at all?
 - Are there different risk profiles?
- To whom?
 - To regulator or individuals, or both?
 - Do you proactively notify financial institutions and credit bureaus? (assess privacy obligations)
- How is notice given?
 - Telephone first?
 - Individual letters
 - Public advertisements

Crisis Management

- When do you give notice?
 - Interference with police or internal investigation
 - Statutory requirements? (Ontario PHIPA)
- What goes in the notice?
 - All the descriptive information plus...
 - Will credit monitoring be offered?
 - To everyone? Or only to those who ask?
 - Do you promise to indemnify loss?
- Do you establish a telephone line or call centre?
 - Are scripts and customer relations staff adequate?

Prevention

- Fundamental
 - “Holistic personal information management” (PIAs and TRAs)
 - Accountability and reporting systems (threats should be known and remedied)
 - Collect only “necessary” personal information for “reasonable” purposes (compliance obligation)
- Organizational and administrative
 - Perform background checks on appropriate personnel (subject to legal constraints)
 - Train personnel and reinforce duties
 - Enforce and audit codes, policies and practices

Prevention

- Physical
 - Add a photo element to ID cards, and name badges
 - Surveillance (subject to legal constraints)
 - Keep hard copy personal information in locked files
- Technical
 - Develop effective encryption systems
 - Keep pace with security standards
- Legal
 - Audit third-party “agent” relationships

DATA BREACH RESPONSE - A Multidisciplinary Perspective

Dan Michaluk of Hicks Morley
djm@hicksmorley.com
<http://danmichaluk.wordpress.com>
(416) 864-7253

David Malamed of Grant Thornton LLP
dmalamed@GrantThornton.ca
(416) 360 -3382
