

Hicks  
Morley

# ADVANTAGE

Your resource for Continuing  
Professional Development

## Responding to Data Breaches

March 25, 2015

accredited  
**CPD**

# **Better breach response – how to be good when things go bad**

Ian Dick

Dan Michaluk

# Better breach response

- The Rules of Professional Conduct
- The basis for good breach response
- Incident response planning
- Notification, harm mitigation and risk management

Responding to Data Breaches

March 25, 2015

Hicks  
Morley

# Rules of Professional Conduct

- Rule 3.2-2 – shall be honest and candid (breach reporting duty?)
- Rule 3.3-1 – shall hold in strict confidence
- Rule 3.5-2 – shall care of a client's property as a careful and prudent owner would...

# Why have a formal, written plan?

- Breaches are best managed as crises
- This means
  - Time is of the essence
  - Organizational behaviour can be problematic
- Also
  - Formal incident response plans are required by recognized data security standards

# The basis for good breach response

- Good records management
  - Records classified in accordance with sensitivity
  - Records with personal information tagged
- Strong logging of system activity
- Security intelligence and periodic vulnerability assessments
- Strong vendor contracts (notification, cooperation, control of breach response)

Responding to Data Breaches

March 25, 2015

Hicks  
Morley

# What's in a plan?

- Identification – what is an "incident"
- Escalation – reporting duties and accountabilities
- Role and process definition (typically featuring a multi-disciplinary "breach response team")
  - Assess – gather facts and triage
  - Contain – immediate
  - Investigate – five Ws
  - Manage – liability, public affairs

# What's in a plan?

- Don't forget!
  - Communication norms
  - Recordkeeping
  - Confidentiality



# Identification and escalation

- Internal reporting supports identification
- Make clear that individuals are not to self-assess

*Any individual who knows or suspects that personal information in the company's custody has been lost or stolen or accessed, disclosed, copied, used or modified without authorization must immediately report the incident to [who] [how].*

# Identification and escalation

- Other means of identification
  - Internal security analysis (network and system analysis is becoming the norm)
  - External reports (police, customers, credit card companies and others)

# The incident response team

- Privacy office
- Information security / corporate security
- Legal
- Risk management
- Communications
- Management from affected business (or human resources if employees are affected)

# Experts to retain in advance

- Why?
  - Objectivity can wither in a crises
  - Bench strength may be required
- Who?
  - IT forensics
  - Crises communications
  - Legal counsel

# Role of legal counsel

- Control strategic direction
- Identify legal risks and potential liabilities
- Input into advocacy
  - Affected persons
  - The media and public
  - Regulators
- Litigation management

# Practice, test, update

- Annual update
  - Plans should, in general, be scenario-neutral
  - Update based on external and internal analysis
  - From new contact information to new procedure
- Tests / fire drills
  - Identify flaws in detection capability
  - Develop tactical IT skills required for correction
  - Discover data gaps and other problems
- Garner decision-making confidence
- Can be an intervention that supports change

## Notification and remediation

- Outside the health sector, only under Alberta legislation currently (S-4 will amend PIPEDA)
- But foreign laws will often apply (and notifying half of an affected population does not work)
- Notification may be required by a common law duty if harm is reasonably foreseeable
- Notification may be desirable b/c people will find out and you can't tolerate the justification process

# Notification and remediation

- What happened (with identification of personal information elements)
- What you've done to contain it
- Contact information
- Consider
  - An apology
  - Telling people where to get help
  - Making a protective offer



# **Better breach response – how to be good when things go bad**

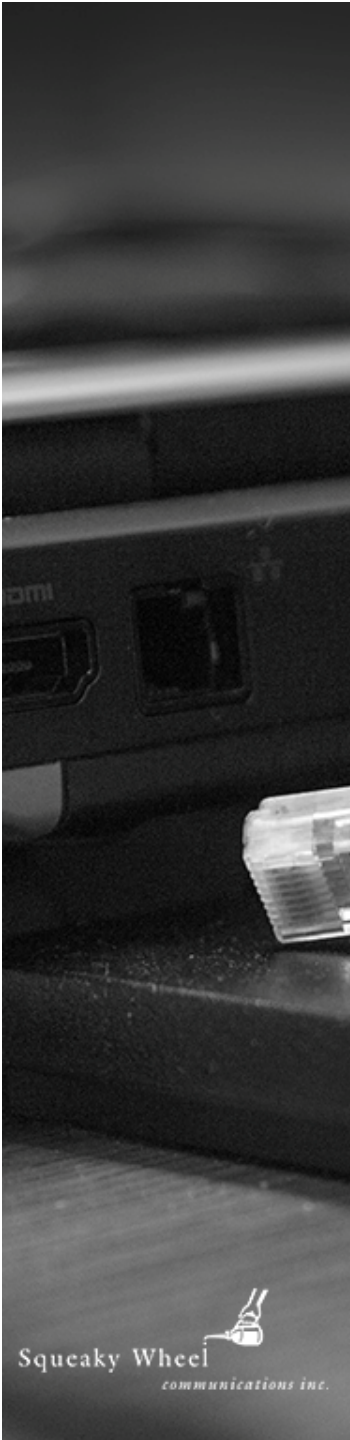
Ian Dick

Dan Michaluk

# Communicating a Data Breach

March 25, 2015  
Karen Gordon  
Squeaky Wheel Communications Inc.

Squeaky Wheel   
*communications inc.*



**It Gets Worse: The Newest  
Sony Data Breach Exposes  
Thousands Of Passwords**

*-Buzzfeed News, Dec. 4, 2014*

**Target Shares Tumble  
As Retailer Reveals  
Cost Of Data Breach**

*-Forbes, Aug 5, 2014*

**Mayor Rob Ford's  
privacy breached,  
hospital says**

*-The Star, Oct 16 2014*

**Neiman Marcus Hackers  
Set Off 60,000 Alerts  
While Bagging Credit  
Card Data**

*-Bloomberg Business, Feb .21, 2014*



# Communications Steps

- Assess
- Report
- Notify
- Communicate
- Monitor



# You need a plan

- Positioning
- Audiences
- Key Messages
- Spokespeople
- Contentious issues
- Tactics and Timing

# Communication Tools

- ▶ Emails
- ▶ Letters
  - ▶ Registered/courier
  - ▶ Bulk mail
- ▶ Phone calls
- ▶ Newspaper ads
- ▶ News releases
- ▶ Website
- ▶ 1-800 line

# Things to think about

- ▶ Can you answer the questions?
- ▶ Long term effect on your brand
- ▶ Your audience
- ▶ What did you know and when?
- ▶ Spokesperson

# Karen Gordon

416.699.1624 p  
416.997.9478 m

Visit our new website at [www.squeakywheel.biz](http://www.squeakywheel.biz)  
Follow me on Twitter at [@squeakywheelcom](https://twitter.com/squeakywheelcom)





# Questions

Ian Dick

Dan Michaluk

Karen Gordon

Hicks  
Morley

# ADVANTAGE

Your resource for Continuing  
Professional Development

## Responding to Data Breaches

March 25, 2015

accredited  
**CPD**