Privacy – what every auditor should know

Malcolm Crompton, Managing Director, Information Integrity Solutions Pty Ltd
Souella Cumming, Partner, KPMG

13 November 2012

INFORMATION INTEGRITY SOLUTIONS

The Institute of Internal Auditors New Zealand

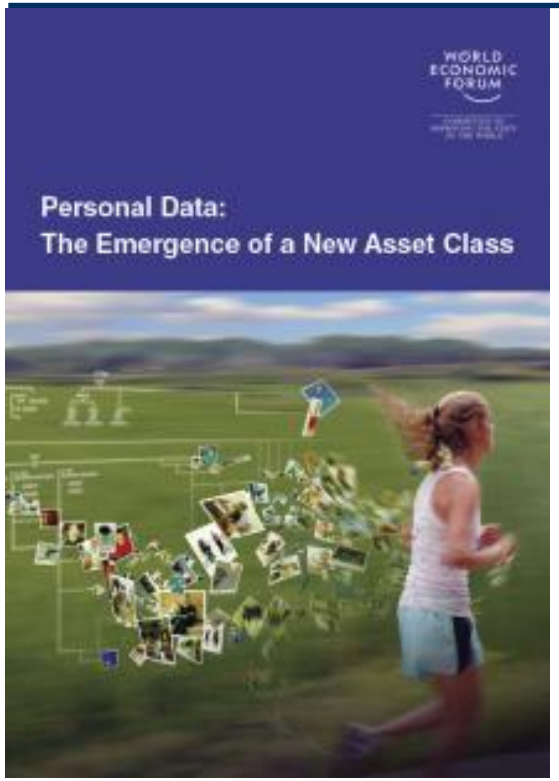
ERNST & YOUNG
Quality In Everything We Do

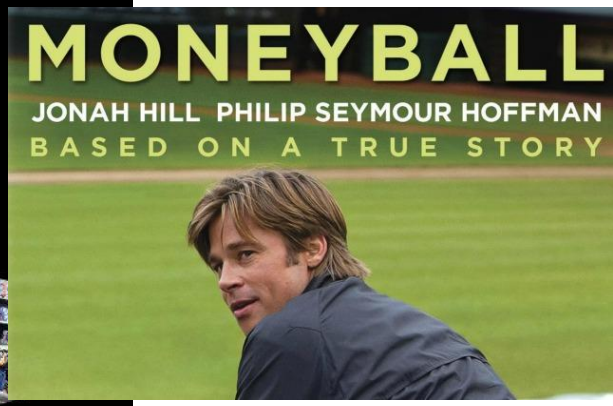
KPMG

Overview

- Current environment/context
  - Data as asset
  - Data as liability
- Data breach could happen to anyone
- ACC – facts and findings
- Implications for internal auditors

Data as asset





ACXIOM®

Real Analytics for facebook®

"As some put it, ***personal data will be the new 'oil' – a valuable resource of the 21st century****. It will emerge as a new asset class touching all aspects of society ... Stakeholders will need to embrace the uncertainty, ambiguity and risk of an emerging ecosystem.*
– World Economic Forum (2011)

KPMG

INFORMATION INTEGRITY SOLUTIONS

Data as liability

Data may be vulnerable to external parties, who act for fun and/or profit

- 81% of data breaches involved some form of **hacking**
- Most common hacking methods are:
  - Exploitation of default or guessable credentials (55%)
  - Use of stolen login credentials (40%)
- 69% of data breaches involved **malware**

- 97% of breaches were avoidable with basic or intermediate security controls
- 85% of breaches too more than a week to discover

Source: '2012 Data Breach Investigations Report', Verizon, 2012

Globally


THE AUSTRALIAN
LOGIN
SIGN UP
AUSTRALIANIT
Gartner
SYMPOSIUM ITXPO 2012
12 – 15 November
The World's
of CIOs and
Focus. Conne
The New York Times
Business Day
TIME
Business & Mo
BUSINESS
TECH
HEALTH
SCIENCE
Personal Finance
Real Estate
ers Getting Smarter?
NEWS
OPINION
NATIONAL
THE WALL STREET JOURNAL.
ASIA EDITION
Monday, February 7, 2011
Home
World
Asia
China
Exchange
Wall Street
Heard on the Street
TOP STORIES IN
Markets
VISA,
March 31, 20
Brian Krebs
Up to 10 r
Tweet 76
Email article
MARKETS | February 7, 2011
Nasdaq Confirn
Article
Stock Quotes
Enjoy your free s
GET ALL OF WSJ.COM
By DEVLIN BARRETT, JENNY STRA
The company that owns the Nasd
weekend that its computer network had been brok
lets leaders of companies, including board memb
documents.
Rise of the hacktivist: Activists now outsteal the thieves
MARCH 23, 2012 | BY GEOFF DUNCAN
A new report on data breaches finds that hacktivists, not traditional cybercriminals, nabbed 58 percent of stolen data in 2011. Is this a sea-change in attacks, and what does it mean for everyday technology users?
Verizon released its annual Data Breach Investigation Report for 2011, in which it finds that
BLOOMBERG/GETTY IMAGES
THINKSTOCK
repeated incidents of data
Security Fix
Brian Krebs on Computer Security
About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Brian Krebs
SEARCH THIS BLOG
Go
Payment Processor Breach May Be Largest Ever
A data breach last year at Princeton, N.J., payment processor Heartland Payment Systems may have compromised tens of millions of credit and debit card transactions, the company said today.
VISA
MasterCard
Under attack ... Visa and MasterCard. Photo: AFP
INFORMATION INTEGRITY SOLUTIONS

New Zealand


Accident Compensation Corporation NZ slammed over data breach
NZ Privacy Commissioner says ACC displayed "an almost cavalier" attitude towards client information, recommends chang
Hamish Barwick (Computerworld) | 27 Augu
ged user data breach
TVNZ News Weather TV Shows Channels TV Guide TVNZ Onder
ONENEWS
Video NZ News World
ACC makes anoth
Published: 6:21PM Saturday Octob
Email this article Print this article
The Accident Compensation C
someone else, in another brea
Waikato truck driver Bruce Lidd
history in the post along with h
Liddington has been battling the
six months ago at work.
As reported on iTnews earlier today, blogger Keith M
to highly sensitive information - including invoices ar
from self-service kiosks installed by the New Zealand
agency.
The data included invoices issued to the Ministry that
Share
Related Whitepapers
Home / News / Technolog
NZ ministry kn
By Juha Saarinen on Oct 15, 201
Filed under Security
Like 1 Tweet 22
Paula Bennett, NZ minister
Google
Today's Weather Dunedin
20 6
HIGH LOW
Forecast
Otago Daily Times
Online Edition | Friday, 2 November 2012 | 11:03:20
News Sport Entertainment Lifestyle Opinion On Campus
Dunedin Queenstown Lakes Regions National World Australia Political Business Weather Technology
Privacy breaches at Inland Revenue
Home » News » Political
Mon, 29 Oct 2012
News: Politics | Inland Revenue
Share 0 Tweet 0 ShareThis
The Inland Revenue Department had 32 privacy breaches involving the personal information of 6300 people being sent to the wrong person in the past year.
Revenue Minister Peter Dunne said 638 people affected by the most serious breach had been contacted because details like their addresses and tax numbers had been released.
Not all those affected by every breach would be contacted, however.
information about
LATEST POLITICAL NEWS
Winz report reveals gaping hole in security
Key denies SAS on Afghan 'revenge mission'
Labour law changes announced
Swipe at education system riles teachers
No quick fixes as Govt tackles housing
Privacy breaches at Inland Revenue
Key signals changes to free up housing land
Crown signs $50m in Treaty deals
more politics >>
KPMG
INFORMATION INTEGRITY SOLUTIONS

Cost of data breach

- Overall financial burden:
  - US – $5.5 million per organisation
  - Australia – $2.16 million
- Lost business costs due to customer turnover and diminished goodwill:
  - US – $3 million per organisation
  - Australia – $840,000
  - Industries with highest turnover rates: technology, consumer and financial services
- Intangibles – **reputation** and **trust**

Source: 2011 Cost of Data Breach Studies: Global and Australia, Ponemon Institute and Symantec, 2012

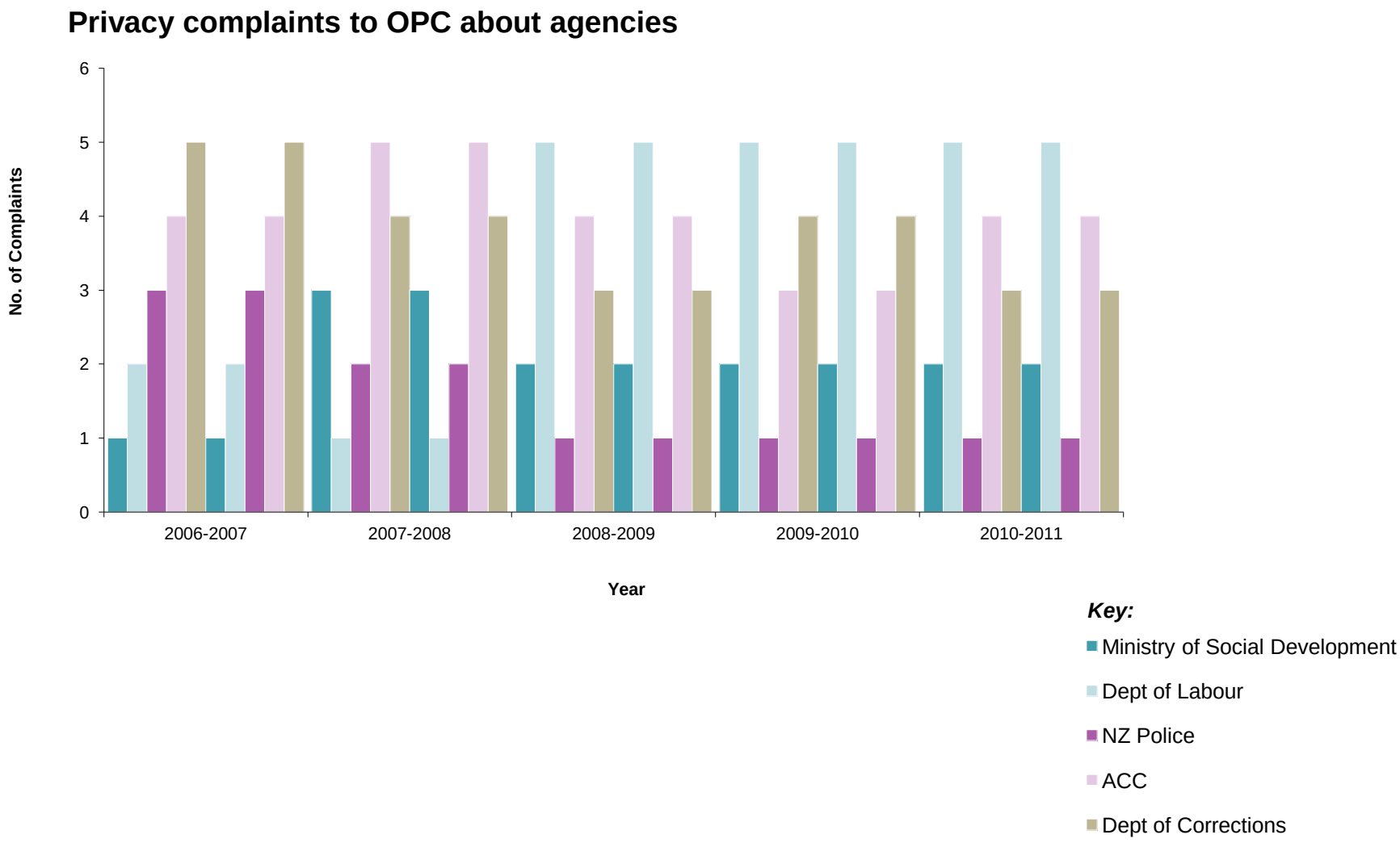
It could happen to anyone

Privacy Commission statistics

- Levels of reported breach have been fairly consistent in recent years
- However...
  - Larger volumes of data
  - Greater visibility – media and general public
  - Multiple incidents reported this year across many agencies
- Reported breach statistics unlikely to settle back to pre-ACC levels

Source:

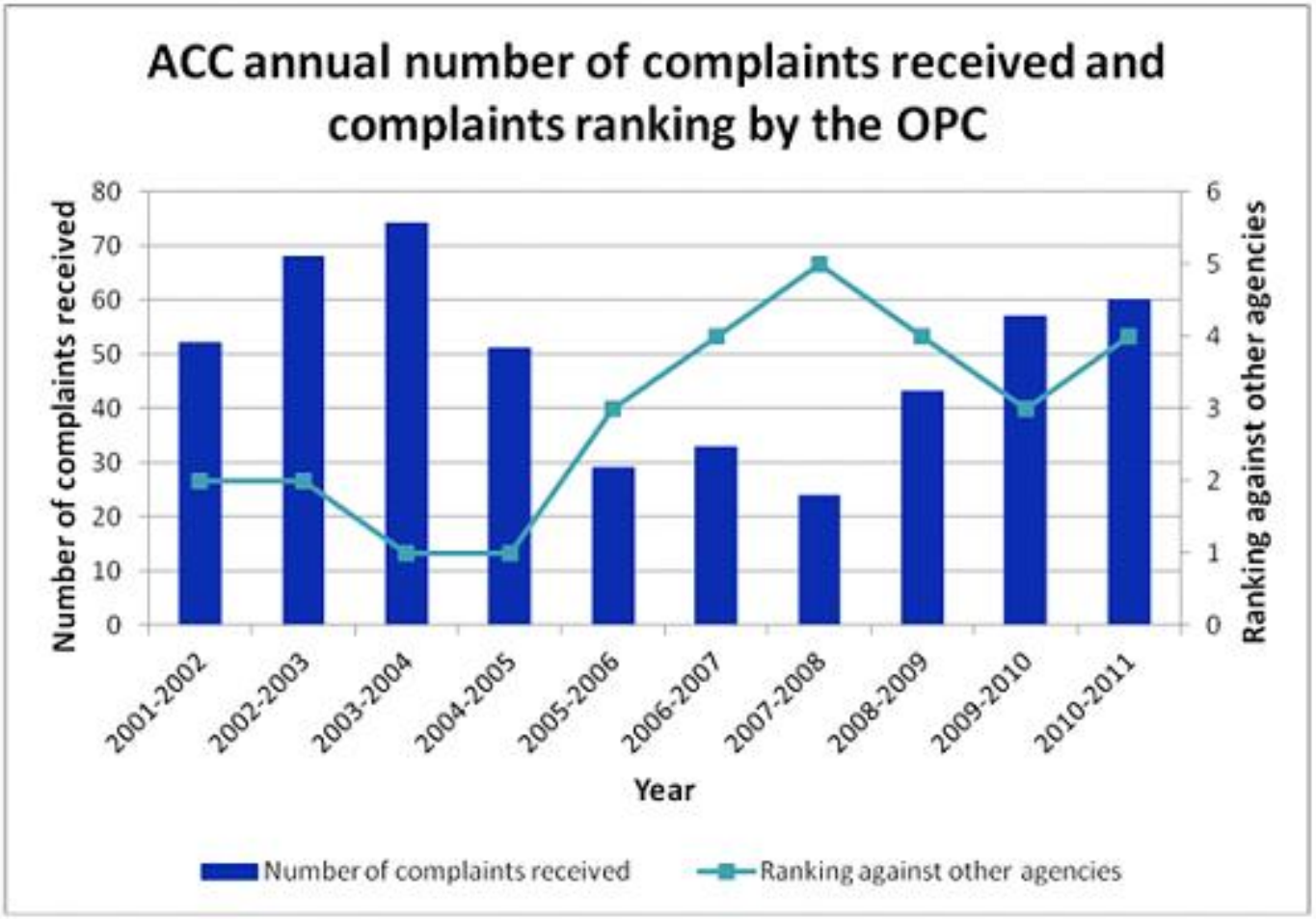
It could happen to anyone



KPMG

INFORMATION INTEGRITY SOLUTIONS

It could happen to anyone



KPMG

INFORMATION INTEGRITY SOLUTIONS

ACC – what happened

05/08/2011	ACC staff member sends email to the Client, inadvertently attaching an internal ACC report containing personal information on 6,748 clients. Over the next two months, the Client raises concerns with ACC regarding its handling of claims and managing personal information.
01/12/2011	Client meets with two senior ACC managers, disclosing the incident.
01/03/2012	Client meets with reporter at Dominion Post. Some information relating to the breach, including re-dated personal information, is provided.
13/03/2012	Media story regarding the breach is made public.
23/03/2012	Independent inquiry is announced.

- "Just a careless mistake?"

ACC – findings

- Data management and privacy is a **whole-of-business issue**
- Cannot address management of personal information in isolation from:
  - Governance
  - Leadership, including privacy strategy
  - Privacy programme
  - ***Culture***
  - Accountability
  - Business processes and systems
  - Safety mechanisms
  - Compliance with the IPPs and the HIPRs

KPMG

INFORMATION INTEGRITY SOLUTIONS

Implications for internal auditors

- **Privacy impact assessment – who knows?**
  - What personal information is collected, stored, used, disclosed?
  - Volumes, nature of the information
- **Understand and assess risk – is it on the risk radar?**
  - What are the risks associated with collecting, storing, using and disclosing personal information?
- **Assess compliance activity – what assurance is provided?**
  - What analysis of reported breaches is undertaken?
  - How effective is the compliance programme?
- **Is a privacy audit on your annual internal audit plan?**

Implications for internal auditors

- **Types of internal audit review/activity**
  - Privacy programme review – appropriateness and effectiveness of organisational approach to privacy
  - Privacy breach monitoring and reporting – completeness and integrity of information reported to the Board/management
  - Information management strategy
  - IT performance and controls including user access management
  - Monitoring and reporting - use of spreadsheets, exchange of information internally and externally
  - Compliance review (separate from or part of legislative compliance review)
  - Risk review
  - Culture review

Summary

"An organisation's data needs to be protected by thorough and effective risk mitigation strategies to the same or higher levels as other vital assets. Without these strategies in place, the organisation is at risk of significant reputational damage."

Souella Cumming commenting on ACC Privacy Breach

"We emphasise the significance of a culture and environment where personal information is valued. This must be supported by an approach to compliance with the privacy principles that is embedded within governance, leadership, business processes and systems."

Malcolm Crompton and Souella Cumming commenting on ACC Privacy Breach

Thank you

Malcolm Crompton
Managing Director
Information Integrity Solutions Pty Ltd
T: + 61 2 8303 2438
E: mcrompton@iispartners.com
W: www.iispartners.com

Souella Cumming
Partner
KPMG
T: + 64 4 816 4519
E: smcumming@kpmg.co.nz
W: www.kpmg.co.nz

INFORMATION INTEGRITY SOLUTIONS

The Institute of Internal Auditors New Zealand

ERNST & YOUNG
Quality In Everything We Do

KPMG