INFORMATION
INTEGRITY
SOLUTIONS

Global Information Governance Summit 2013

"Acclaiming Accountability.
Preaching Best Practices."

Privacy around the world: Developments, challenges and responses

Annelies Moens
Head of Sales and Operations
Information Integrity Solutions

GIGS 2013
Kuala Lumpur, 29 May 2013

INFORMATION
INTEGRITY
SOLUTIONS

About IIS

- ➢ Building trust and privacy through global thought leadership and consultancy work for a range of public and private organisations
- ➢ Services: privacy governance & strategy, privacy impact assessments and audits, regulator, customer & stakeholder engagement, identity management, privacy training…..

Australian Government

AUSTRALIA POST

Microsoft®

CommonwealthBank

ebay™

cisco™

Google Singapore

APEC
Asia-Pacific Economic Cooperation

Building trust and innovative privacy solutions

Overview

- Changing regional and global privacy regulation
- Privacy challenges
- Case study: Accident Compensation Corporation, New Zealand
- Framework for good privacy management

Strengthening Trust

- Explosive growth in the quantity and quality of personal data has created significant opportunity to create new forms of economic and social value

… yet

- Individuals are beginning to lose trust in how organisations and governments are using data about them

WORLD ECONOMIC FORUM

Industry Agenda

Rethinking Personal Data: Strengthening Trust

Prepared in collaboration with The Boston Consulting Group

Source: World Economic Forum, Rethinking Personal Data: Strengthening Trust **(2013)**

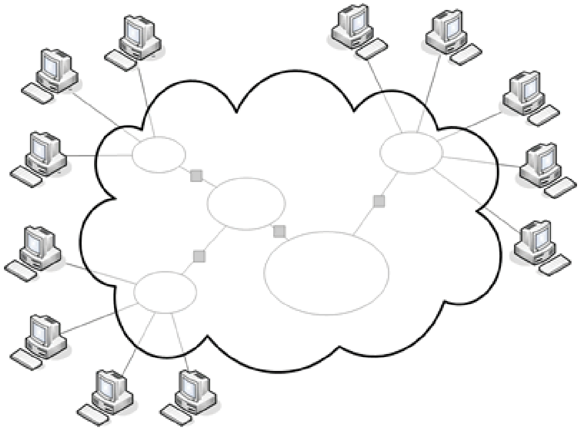
Asia-Pacific – Recent Developments

Country	Law / Guideline	In Force	Coverage
Malaysia	Personal Data Protection Act, 2010	Not yet	Private sector, in commercial transactions
Singapore	Personal Data Protection Act 2012	Yes, in phases	Private sector
Vietnam	Law on Protection of Consumer's Rights, 2011	Yes	Private sector, in commercial transactions
Taiwan	Personal Data Protection Act, 2010	Yes	Public and private sectors
India	Information Technology Act, 2000 and IT Rules, 2011	Yes	Private sector
South Korea	Personal Data Protection Act, 2011	Yes	Public and private sectors
Philippines	Data Privacy Act of 2012	Yes	Public and private sectors
Hong Kong	Personal Data (Privacy)(Amendment) Ordinance 2012	Yes, in phases	Public and private sectors
China	Information Security Technology – Guide for Personal Information Protection within Public and Commercial Information Systems	Yes	Private sector

APEC

- Finalisation of the Cross-Border Privacy Rules (CBPR) system for APEC member economies
- System to ensure that a company’s privacy practices meet established standards for the protection of personal information
- First participant of CBPR is USA, then Mexico, with more to follow, including Japan this year
- Discussions to foster interoperability with the EU’s Binding Corporate Rules (BCR)

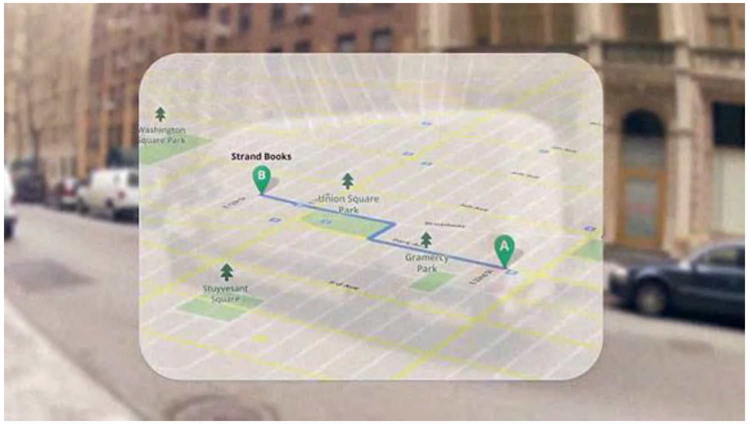
INFORMATION INTEGRITY SOLUTIONS



Privacy Challenges

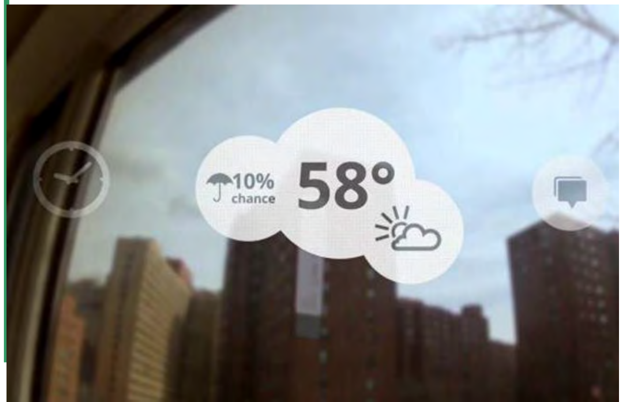
Building trust and innovative privacy solutions

Private Surveillance - Google Glasses



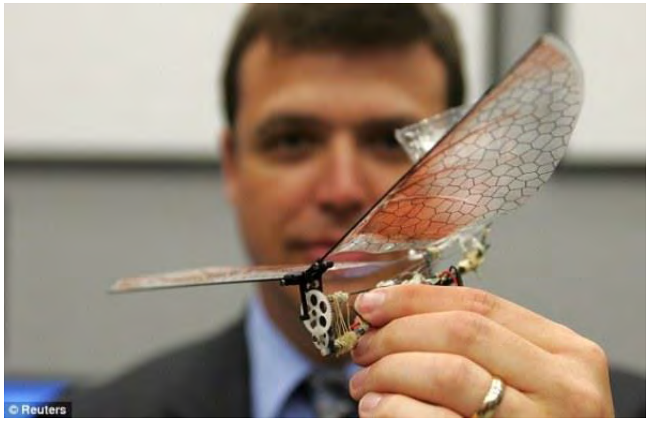
What is it?

- Wearable computer with head-mounted display
- Features and functions:
  - Communication (via connection with smartphone)
  - Web browsing and operations
  - Takes photos and records 720p HD video
  - Augmented reality (overlay information onto real world)



Privacy challenges

- Surreptitious recording
- Ubiquitous surveillance
- Collection of private and sensitive information
- Data control and ownership



Private surveillance - Drones

What is it?

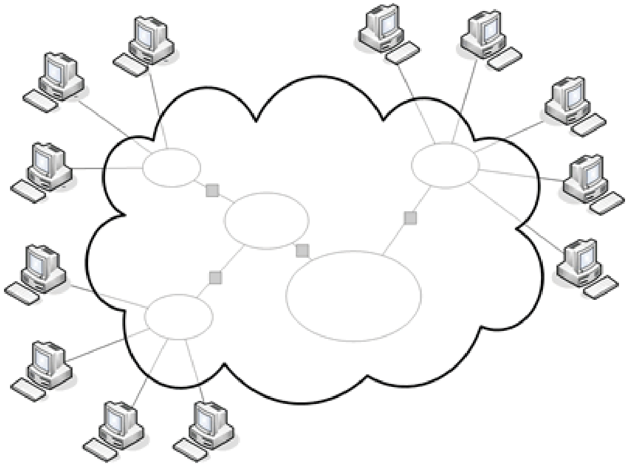
- ➢ Unmanned aerial vehicle (UAV) – flying machine operated remotely and equipped with sensors
- ➢ Functions:
  - ❑ Military
  - ❑ Exploration
  - ❑ Search and rescue
  - ❑ **Law enforcement surveillance**
  - ❑ **Paparazzi**
  - ❑ **Personal use**
  - ❑ Etc

Privacy challenges

- Ease and availability
- Ubiquitous surveillance
- Potential for abuse

INFORMATION INTEGRITY SOLUTIONS

Cloud Computing



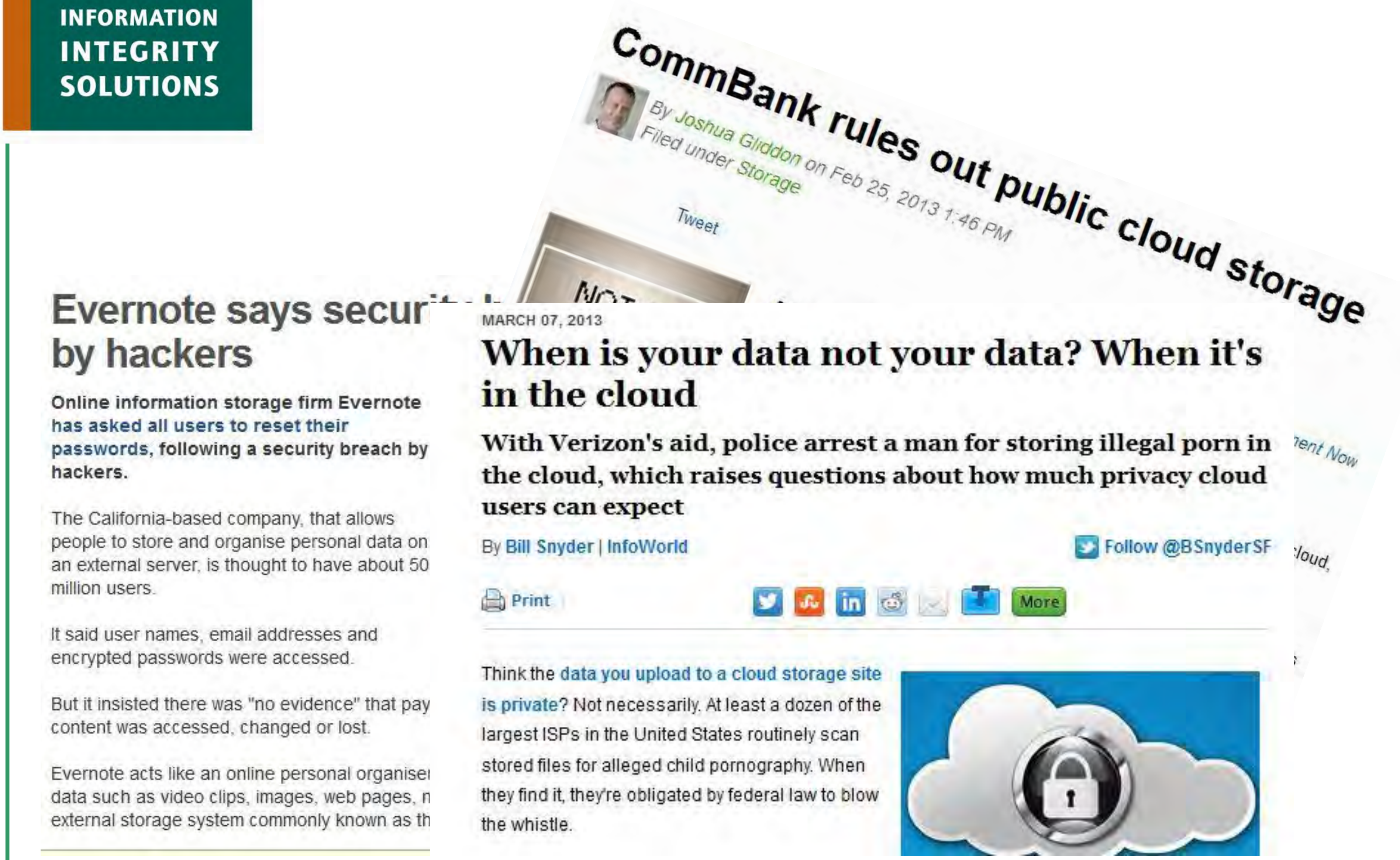
Building trust and innovative privacy solutions

What is cloud computing?

On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use

Why engage a CSP?

- Connecting with multiple devices, business agility and cost-cutting were the top three reasons cited for adopting cloud services (TNS)
- In a recent survey of 674 IT and business executives at organisations across a range of industries and countries (KPMG):
  - ❑ 70% agree that cloud computing is delivering efficiencies and cost savings
  - ❑ Cloud adopters are also starting to focus on business process transformation, in addition to cost and speed benefits



CommBank rules out public cloud storage

By Joshua Gliddon on Feb 25, 2013 1:46 PM
Filed under Storage

Tweet

ent Now

cloud,

Evernote says securi

by hackers

Online information storage firm Evernote has asked all users to reset their passwords, following a security breach by hackers.

The California-based company, that allows people to store and organise personal data on an external server, is thought to have about 50 million users.

It said user names, email addresses and encrypted passwords were accessed.

But it insisted there was "no evidence" that pay content was accessed, changed or lost.

Evernote acts like an online personal organise data such as video clips, images, web pages, n external storage system commonly known as th

MARCH 07, 2013

When is your data not your data? When it's in the cloud

With Verizon's aid, police arrest a man for storing illegal porn in the cloud, which raises questions about how much privacy cloud users can expect

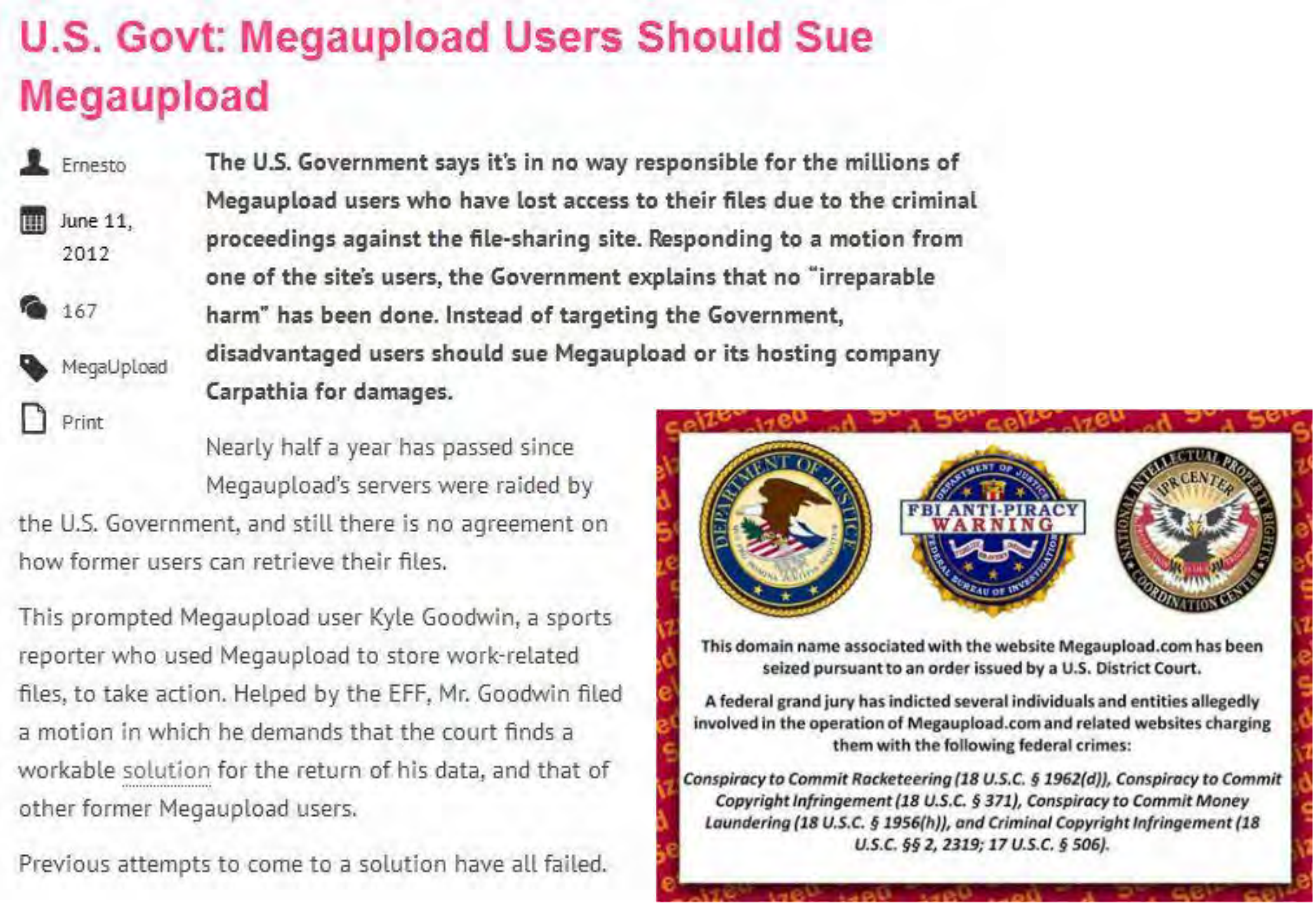
By Bill Snyder | InfoWorld

Follow @BSnyderSF

Print

More

Think the data you upload to a cloud storage site is private? Not necessarily. At least a dozen of the largest ISPs in the United States routinely scan stored files for alleged child pornography. When they find it, they're obligated by federal law to blow the whistle.



U.S. Govt: Megaupload Users Should Sue Megaupload

Ernesto

June 11, 2012

167

MegaUpload

Print

The U.S. Government says it's in no way responsible for the millions of Megaupload users who have lost access to their files due to the criminal proceedings against the file-sharing site. Responding to a motion from one of the site's users, the Government explains that no "irreparable harm" has been done. Instead of targeting the Government, disadvantaged users should sue Megaupload or its hosting company Carpathia for damages.

Nearly half a year has passed since Megaupload's servers were raided by the U.S. Government, and still there is no agreement on how former users can retrieve their files.

This prompted Megaupload user Kyle Goodwin, a sports reporter who used Megaupload to store work-related files, to take action. Helped by the EFF, Mr. Goodwin filed a motion in which he demands that the court finds a workable solution for the return of his data, and that of other former Megaupload users.

Previous attempts to come to a solution have all failed.

DEPARTMENT OF JUSTICE
FBI ANTI-PIRACY WARNING
FEDERAL BUREAU OF INVESTIGATION
NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER
IPR CENTER

This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by a U.S. District Court.

A federal grand jury has indicted several individuals and entities allegedly involved in the operation of Megaupload.com and related websites charging them with the following federal crimes:

Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)), Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371), Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).

Preliminary privacy considerations

Types of data and privacy policies:

1. How sensitive or critical to your business is the data that the CSP will be processing/hosting?
2. Is the disclosure/transfer of personal information to the CSP authorised by your customers?
3. Whose privacy policy is the data subject to once outsourced – your business or the CSP's privacy policy? Who owns the data once with the CSP?

Privacy risks

Location and retention of data	Transferring data	Changing provider
Location of data and backups • Politically and environmentally stable regions? • Legal jurisdiction of data • How does the CSP know where the data is? • With other clients' data?	Technical glitches • What happens when the data cannot be accessed or retrieved from the cloud service provider due to technical or other difficulties?	Unforeseen events • What happens when CSP is shut down? • How is operational change handled - CSP bankrupt, sold, merged • How is a disaster/ hacking managed?
Protection and Security • Encrypted whilst stored? • Who controls the encryption keys? • Physical security	Protection and Security • Encrypted in transfer? • Who controls the encryption keys?	Updates • Can upgrades to software or other services be refused?
Retention • What are the data retention policies?	Subcontractors • Does the CSP use third party subcontractors?	Portability • Can the data be easily relocated?

10 safeguards

1. Read the contract and terms of service very closely and clarify any ambiguous provisions
2. Add cloud computing to your outsourcing and/or offshoring risk management frameworks
3. Ensure you are not violating any law or policy by putting personal information in the cloud
4. Clarify the rights of access, correction and deletion
5. Find out where and how the data will be kept
6. Ensure that the CSP passes all obligations it must meet under the contract to any subcontractors
7. Determine liability and accountability – what happens when things go wrong?
8. Have back-ups
9. Establish your own security measures
10. Maintain assurance and audit processes

Model contract

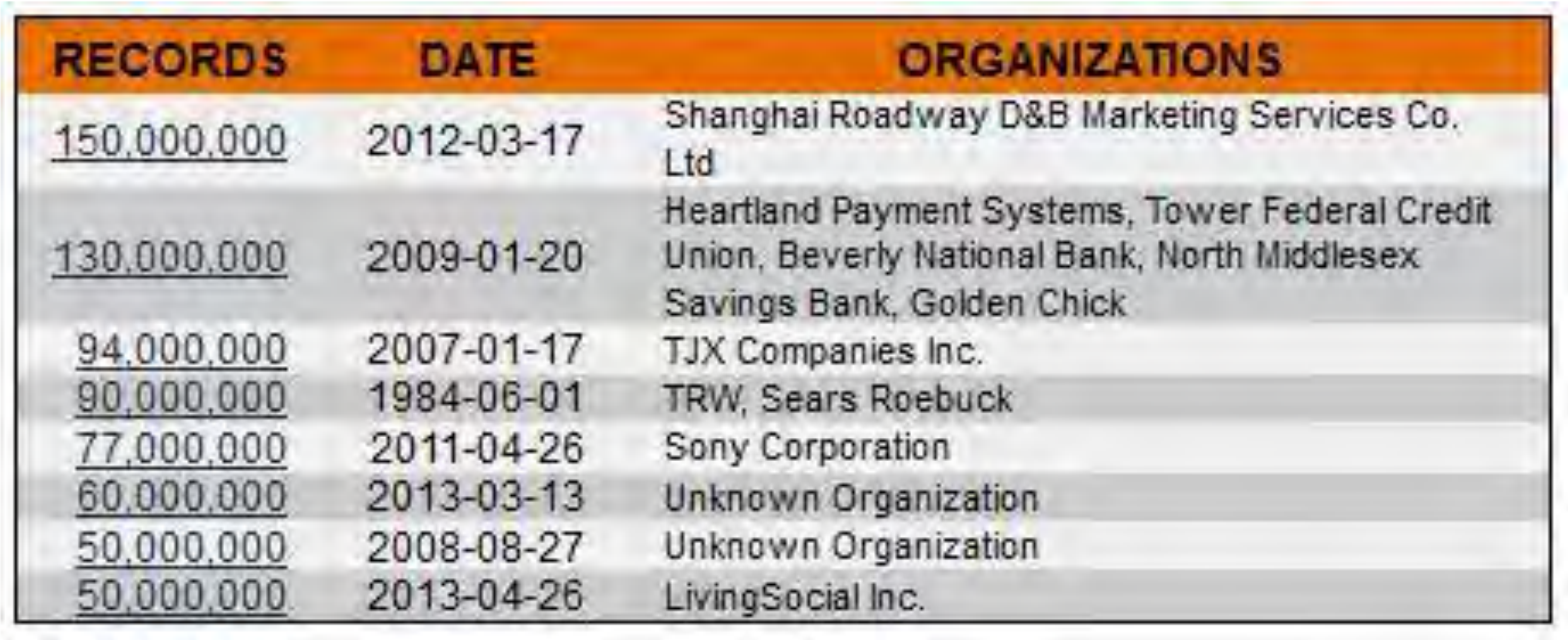
New Zealand Cloud Computing Code of Practice	
Corporate Identity	Service level agreement and support
Ownership of Data	Data breach notification
Security	Data transportability
Data Location/Geographic Diversity	Data formats
Data Access and Use	Business Continuity
Back up and Maintenance	Ownership of application

INFORMATION INTEGRITY SOLUTIONS

Data Breaches

Building trust and innovative privacy solutions

Data breaches are pervasive



RECORDS	DATE	ORGANIZATIONS
150,000,000	2012-03-17	Shanghai Roadway D&B Marketing Services Co. Ltd
130,000,000	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank, North Middlesex Savings Bank, Golden Chick
94,000,000	2007-01-17	TJX Companies Inc.
90,000,000	1984-06-01	TRW, Sears Roebuck
77,000,000	2011-04-26	Sony Corporation
60,000,000	2013-03-13	Unknown Organization
50,000,000	2008-08-27	Unknown Organization
50,000,000	2013-04-26	LivingSocial Inc.

***Source: DataLossDB, Largest Incidents* (2013)**

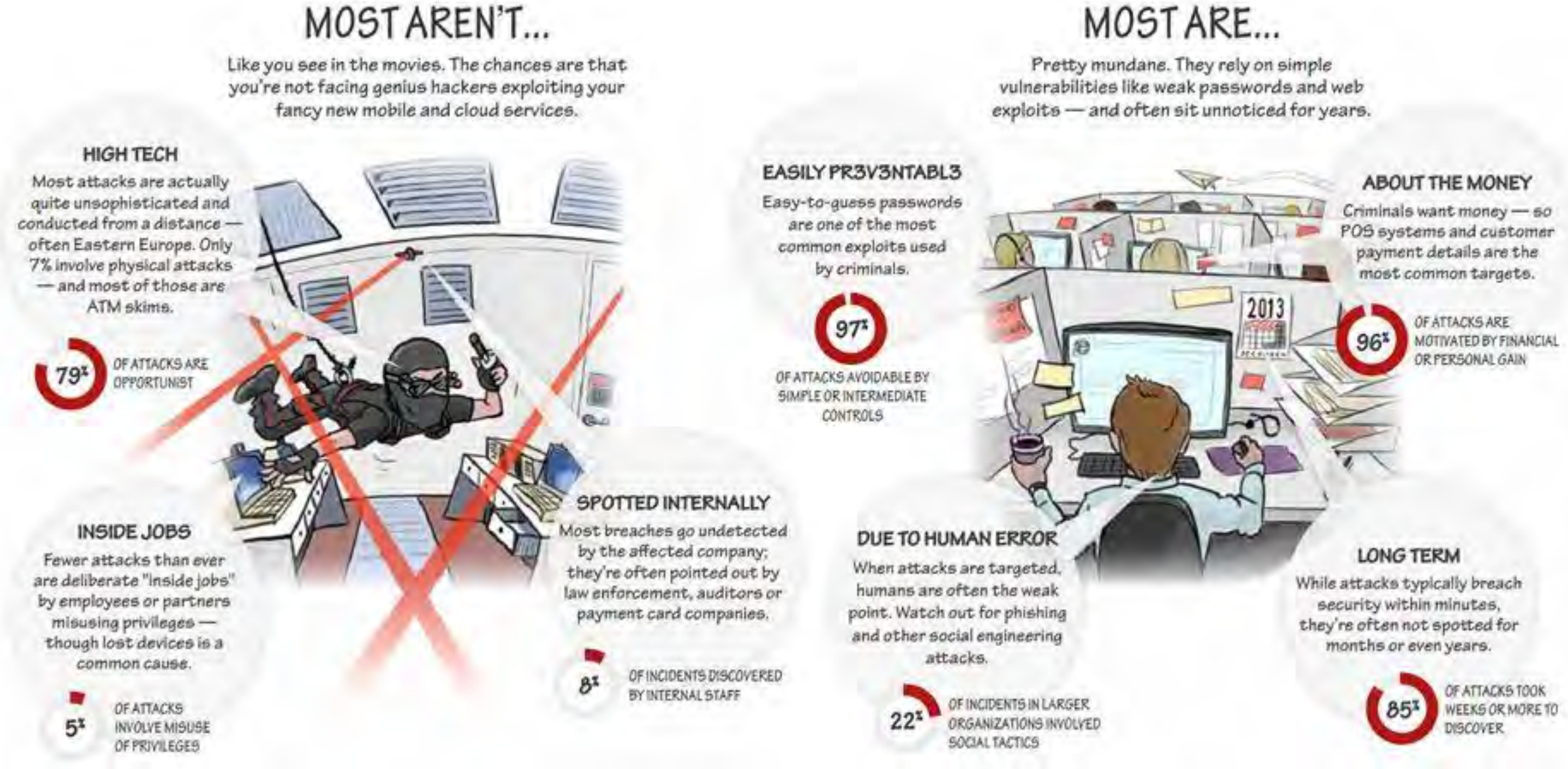
INFORMATION INTEGRITY SOLUTIONS

Impact of a data breach

- Data breaches have increased in severity and frequency, but organisations lack tools to detect and respond
- Malicious data breaches cost 60% more than non-malicious ones, per organisation ($840,000 v $500,000)
- Reported reasons for breaches:
  - ❑ Non-malicious – Lack of in-house expertise (50%), inadequate security processes (37%)
  - ❑ Malicious – Lack of in-house expertise (64%), inadequate forensic capabilities (47%)

Source: Ponemon Institute, The Post Breach Boom **(2013)**

Internal threats



MOST AREN'T...

Like you see in the movies. The chances are that you're not facing genius hackers exploiting your fancy new mobile and cloud services.

HIGH TECH

Most attacks are actually quite unsophisticated and conducted from a distance — often Eastern Europe. Only 7% involve physical attacks — and most of those are ATM skims.

79% OF ATTACKS ARE OPPORTUNIST

INSIDE JOBS

Fewer attacks than ever are deliberate "inside jobs" by employees or partners misusing privileges — though lost devices is a common cause.

5% OF ATTACKS INVOLVE MISUSE OF PRIVILEGES

SPOTTED INTERNALLY

Most breaches go undetected by the affected company; they're often pointed out by law enforcement, auditors or payment card companies.

8% OF INCIDENTS DISCOVERED BY INTERNAL STAFF

MOST ARE...

Pretty mundane. They rely on simple vulnerabilities like weak passwords and web exploits — and often sit unnoticed for years.

EASILY PR3V3NTABL3

Easy-to-guess passwords are one of the most common exploits used by criminals.

97% OF ATTACKS AVOIDABLE BY SIMPLE OR INTERMEDIATE CONTROLS

ABOUT THE MONEY

Criminals want money — so POS systems and customer payment details are the most common targets.

96% OF ATTACKS ARE MOTIVATED BY FINANCIAL OR PERSONAL GAIN

DUE TO HUMAN ERROR

When attacks are targeted, humans are often the weak point. Watch out for phishing and other social engineering attacks.

22% OF INCIDENTS IN LARGER ORGANIZATIONS INVOLVED SOCIAL TACTICS

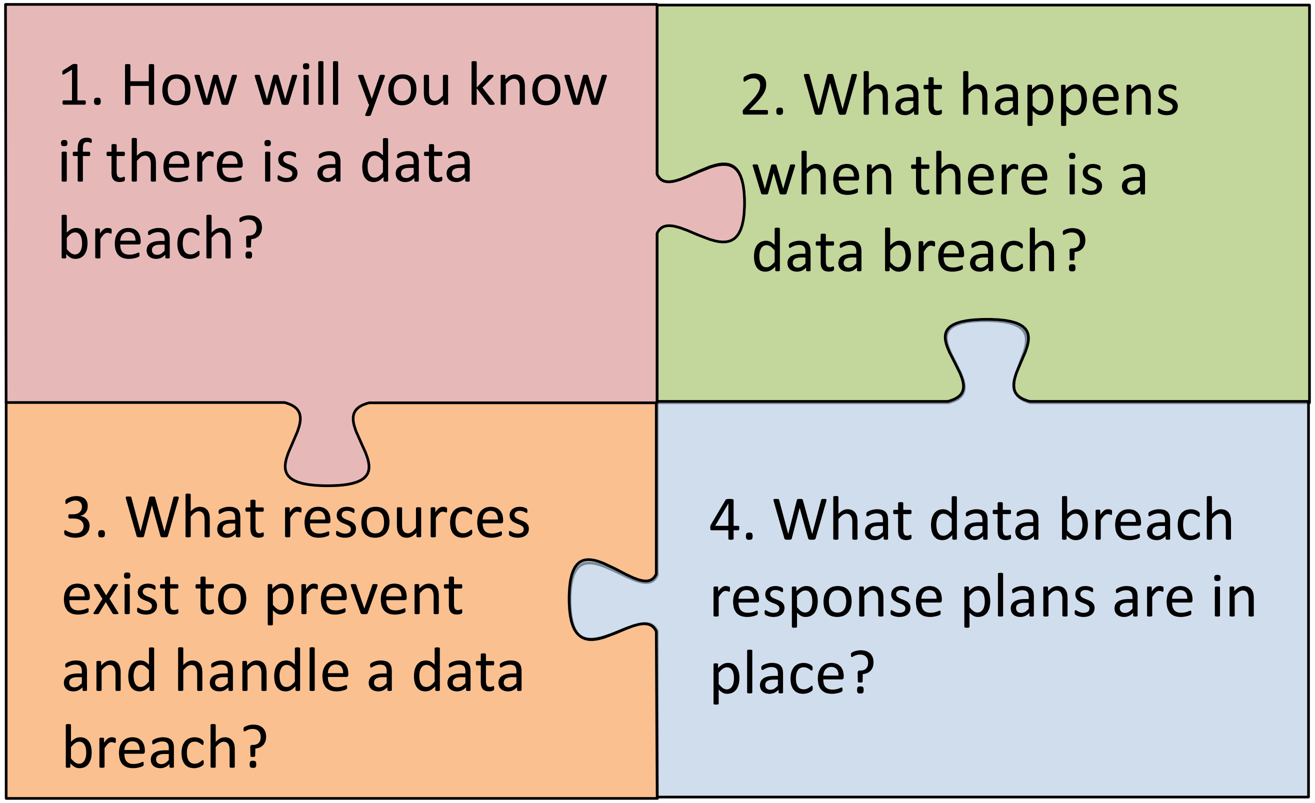
LONG TERM

While attacks typically breach security within minutes, they're often not spotted for months or even years.

85% OF ATTACKS TOOK WEEKS OR MORE TO DISCOVER

***Reproduced with permission from Verizon – Verizon 2012 Data Breach Investigations Report* (2012)**

Data breaches



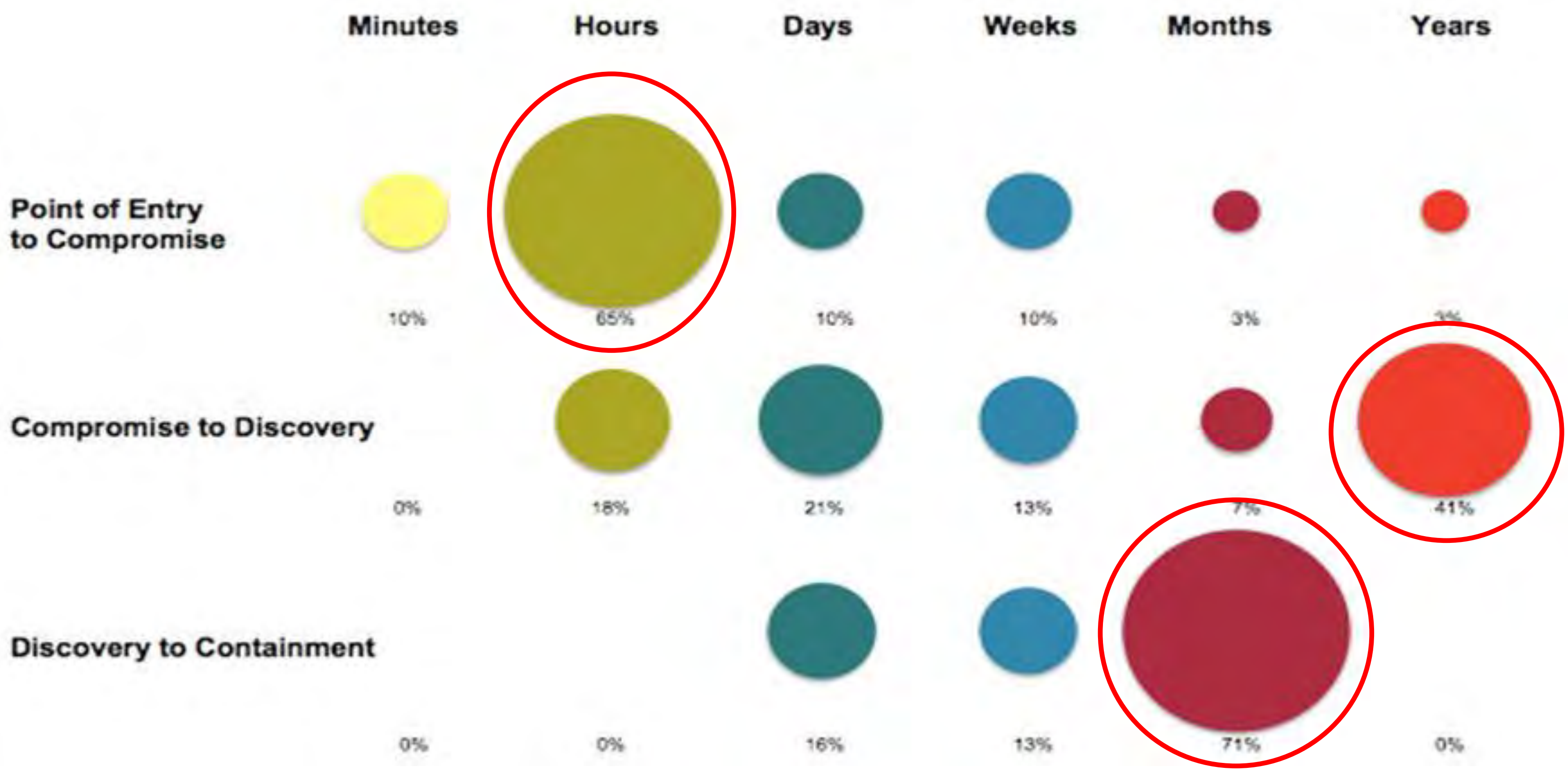
1. How will you know if there is a data breach?

2. What happens when there is a data breach?

3. What resources exist to prevent and handle a data breach?

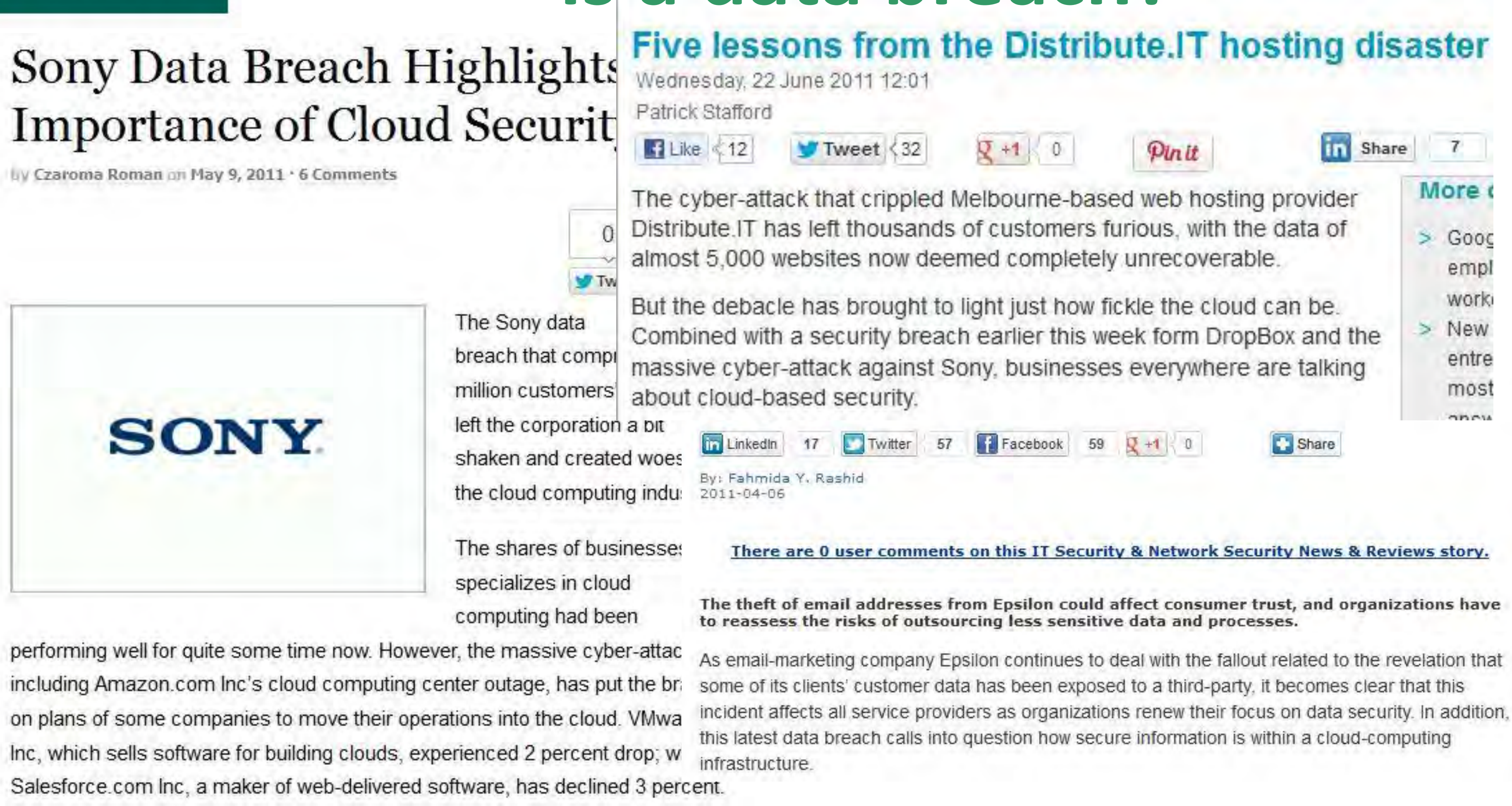
4. What data breach response plans are in place?

1. How will you know if there is a data breach?



Reproduced with permission from Verizon – Verizon 2012 Data Breach Investigations Report (2012)

2. What happens when there is a data breach?



Sony Data Breach Highlights Importance of Cloud Securit

by Czaroma Roman on May 9, 2011 · 6 Comments

The Sony data breach that compr million customers left the corporation a bit shaken and created woes the cloud computing indu

The shares of businesse specializes in cloud computing had been performing well for quite some time now. However, the massive cyber-attac including Amazon.com Inc's cloud computing center outage, has put the br on plans of some companies to move their operations into the cloud. VMwa Inc, which sells software for building clouds, experienced 2 percent drop; w Salesforce.com Inc, a maker of web-delivered software, has declined 3 percent.

Five lessons from the Distribute.IT hosting disaster

Wednesday, 22 June 2011 12:01

Patrick Stafford

The cyber-attack that crippled Melbourne-based web hosting provider Distribute.IT has left thousands of customers furious, with the data of almost 5,000 websites now deemed completely unrecoverable.

But the debacle has brought to light just how fickle the cloud can be. Combined with a security breach earlier this week form DropBox and the massive cyber-attack against Sony, businesses everywhere are talking about cloud-based security.

By: Fahmida Y. Rashid
2011-04-06

There are 0 user comments on this IT Security & Network Security News & Reviews story.

The theft of email addresses from Epsilon could affect consumer trust, and organizations have to reassess the risks of outsourcing less sensitive data and processes.

As email-marketing company Epsilon continues to deal with the fallout related to the revelation that some of its clients' customer data has been exposed to a third-party, it becomes clear that this incident affects all service providers as organizations renew their focus on data security. In addition, this latest data breach calls into question how secure information is within a cloud-computing infrastructure.

3. What resources exist to prevent and handle a data breach?

- Steps you can take to minimise the likelihood of a data breach:
  - ❑ Privacy by Design in business process and ICT
  - ❑ Privacy Impact Assessments
  - ❑ Privacy in risk management frameworks
  - ❑ Privacy skills development and training
- Check whether your insurer covers the cost of dealing with a data breach and notification
- Consider what your data breach response plan is

4. What data breach response plans are in place?

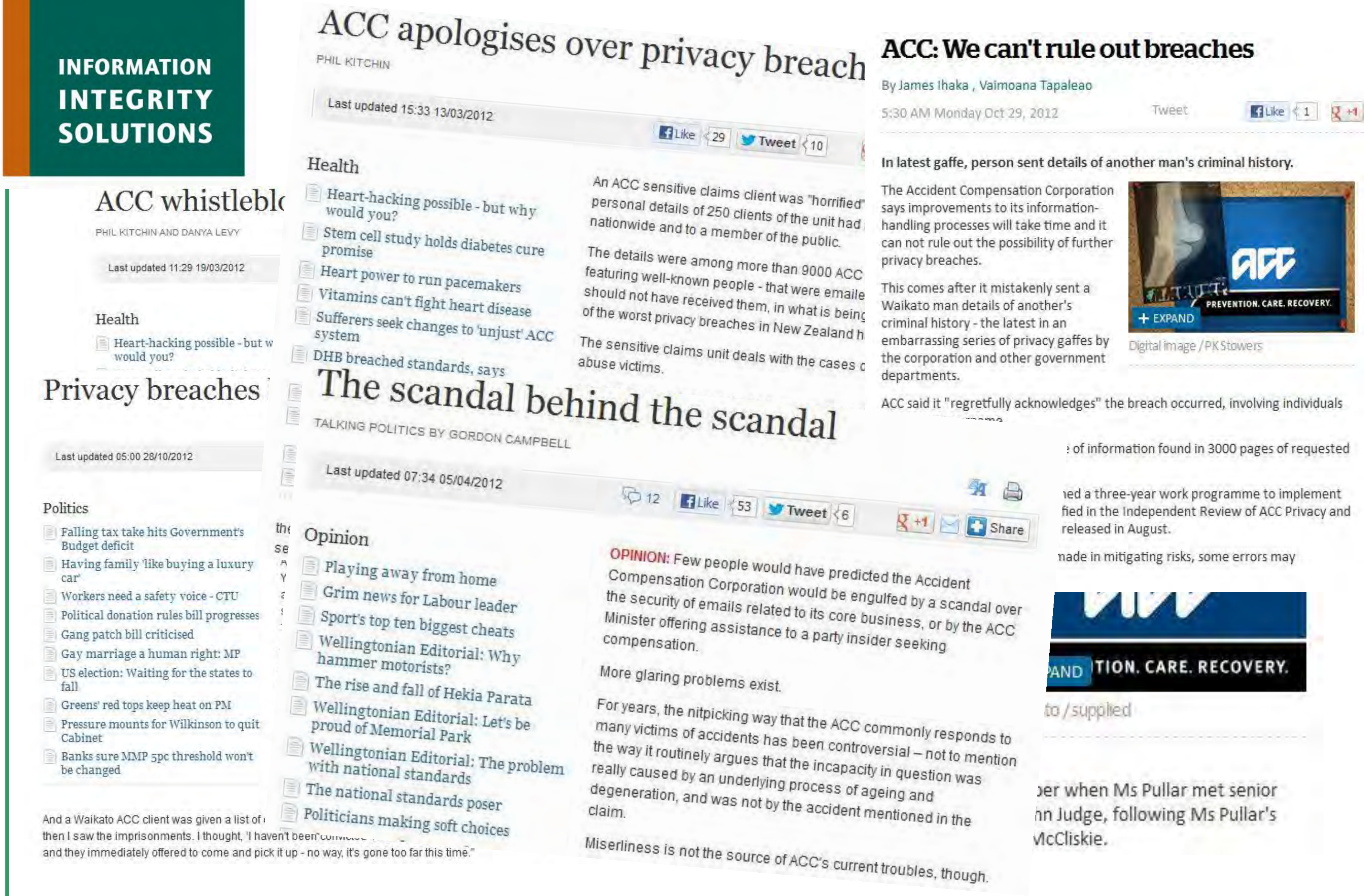
1. Contain the breach and do a preliminary assessment
2. Appoint lead person to manage (internal and/or external) response team
3. Evaluate the risks associated with the breach
4. Consider breach notification
5. Review the incident and take action to prevent future breaches

Case study: ACC

Facts

- 5 August 2011 – email to client with an attachment containing personal information of 6,748 of ACC’s clients
- Recipient became aware on 26 October 2011 and advised ACC on 1 December 2011
- 13 March 2012 breach became public and IIS and KPMG engaged to conduct independent review

INFORMATION
INTEGRITY
SOLUTIONS



ACC apologises over privacy breach

PHIL KITCHIN

Last updated 15:33 13/03/2012

Health

- Heart-hacking possible - but why would you?
- Stem cell study holds diabetes cure promise
- Heart power to run pacemakers
- Vitamins can't fight heart disease
- Sufferers seek changes to 'unjust' ACC system
- DHB breached standards, says

An ACC sensitive claims client was "horrified" personal details of 250 clients of the unit had nationwide and to a member of the public.

The details were among more than 9000 ACC featuring well-known people - that were emaile should not have received them, in what is being of the worst privacy breaches in New Zealand h

The sensitive claims unit deals with the cases c abuse victims.

ACC: We can't rule out breaches

By James Ihaka , Vaimoana Tapaleao

5:30 AM Monday Oct 29, 2012

In latest gaffe, person sent details of another man's criminal history.

The Accident Compensation Corporation says improvements to its information-handling processes will take time and it can not rule out the possibility of further privacy breaches.

This comes after it mistakenly sent a Waikato man details of another's criminal history - the latest in an embarrassing series of privacy gaffes by the corporation and other government departments.

Digital image / PK Stowers

ACC said it "regretfully acknowledges" the breach occurred, involving individuals

: of information found in 3000 pages of requested

ıed a three-year work programme to implement fied in the Independent Review of ACC Privacy and released in August.

ıade in mitigating risks, some errors may

to / supplied

ɔer when Ms Pullar met senior ın Judge, following Ms Pullar's McCliskie.

ACC whistlebl

PHIL KITCHIN AND DANYA LEVY

Last updated 11:29 19/03/2012

Health

- Heart-hacking possible - but w would you?

Privacy breaches

Last updated 05:00 28/10/2012

Politics

- Falling tax take hits Government's Budget deficit
- Having family 'like buying a luxury car'
- Workers need a safety voice - CTU
- Political donation rules bill progresses
- Gang patch bill criticised
- Gay marriage a human right: MP
- US election: Waiting for the states to fall
- Greens' red tops keep heat on PM
- Pressure mounts for Wilkinson to quit Cabinet
- Banks sure MMP 5pc threshold won't be changed

And a Waikato ACC client was given a list of then I saw the imprisonments. I thought, 'I haven't been and they immediately offered to come and pick it up - no way, it's gone too far this time."

The scandal behind the scandal

TALKING POLITICS BY GORDON CAMPBELL

Last updated 07:34 05/04/2012

Opinion

- Playing away from home
- Grim news for Labour leader
- Sport's top ten biggest cheats
- Wellingtonian Editorial: Why hammer motorists?
- The rise and fall of Hekia Parata
- Wellingtonian Editorial: Let's be proud of Memorial Park
- Wellingtonian Editorial: The problem with national standards
- The national standards poser
- Politicians making soft choices

OPINION: Few people would have predicted the Accident Compensation Corporation would be engulfed by a scandal over the security of emails related to its core business, or by the ACC Minister offering assistance to a party insider seeking compensation.

More glaring problems exist.

For years, the nitpicking way that the ACC commonly responds to many victims of accidents has been controversial – not to mention the way it routinely argues that the incapacity in question was really caused by an underlying process of ageing and degeneration, and was not by the accident mentioned in the claim.

Miserliness is not the source of ACC's current troubles, though.

Building trust and innovative privacy solutions

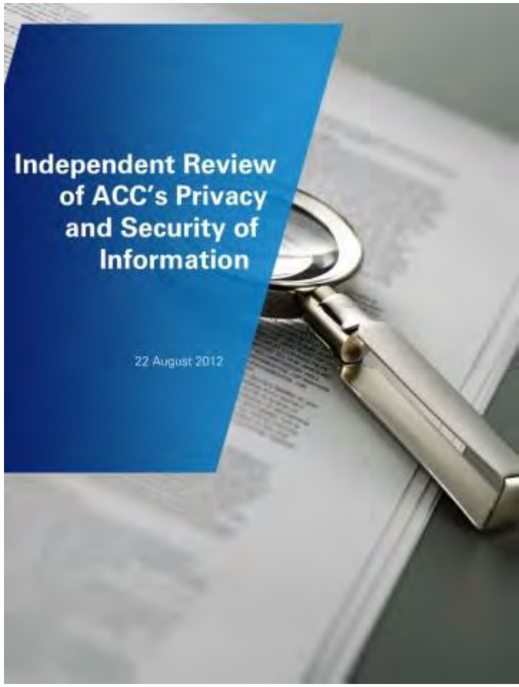
Systemic issues

Breach was a genuine error – but errors are able to happen because of systemic weaknesses within ACC's culture, systems and processes.

- Technology and business practice – spreadsheets and multiple monitors
- Culture – inconsistent respect for personal info
- Privacy Management – lack of accountability

Recommendations

- Breach was a symptom of underlying systematic issues
- Privacy is a **whole-of-agency concern**
  - □ Governance
  - □ Leadership, including privacy strategy
  - □ Privacy programme
  - □ Culture
  - □ Accountability
  - □ Business processes and systems
  - □ Backlog



Independent Review of ACC's Privacy and Security of Information

22 August 2012

Whole-of-agency issue

- Data management and privacy is a **whole-of-agency issue**

"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."	"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."

Lessons learnt

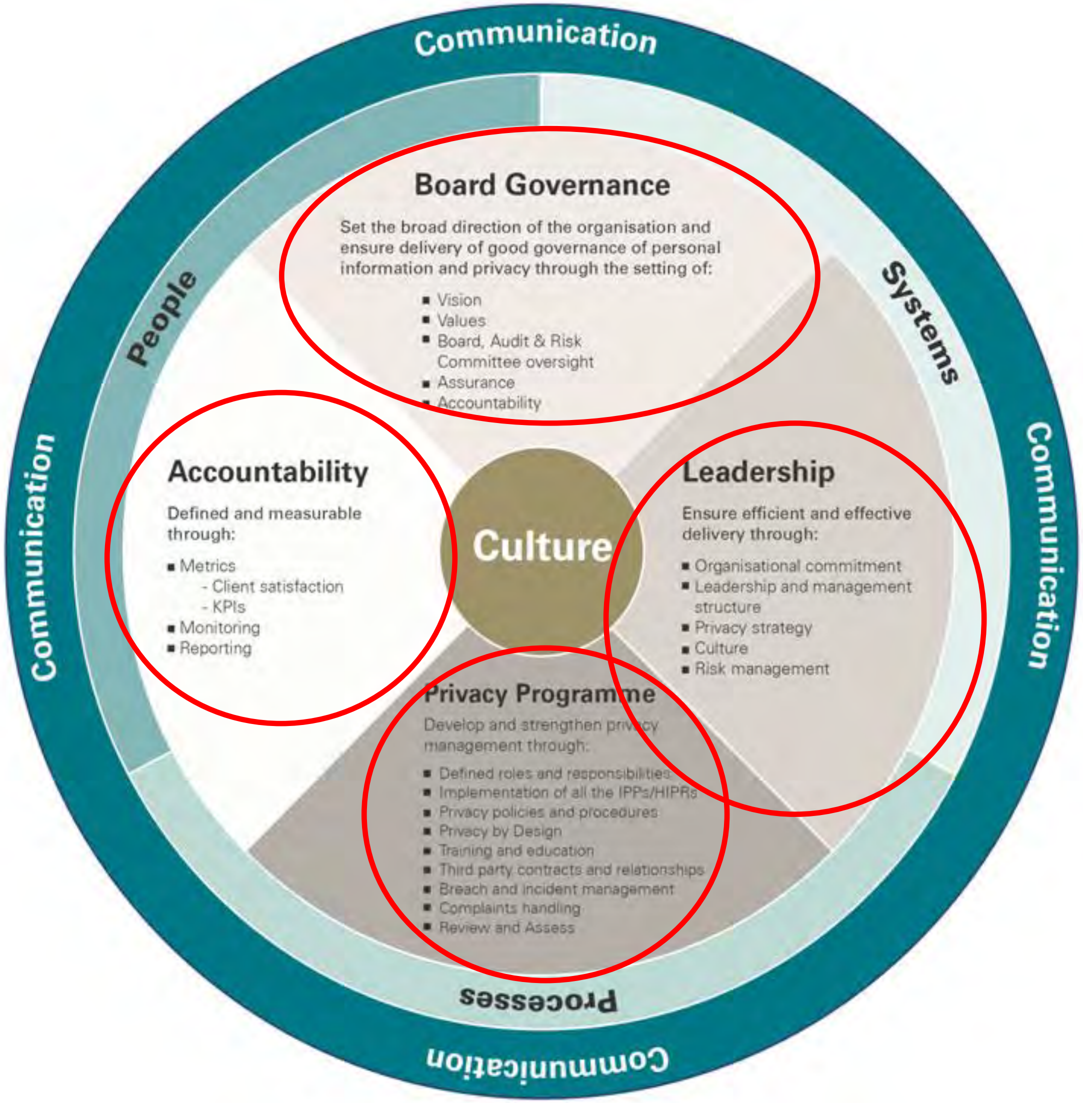
1) Make privacy part of risk management frameworks

2) Having a customer focus and viewpoint helps solve and prevent privacy issues

3) Treat personal information and other information as an asset – if it is not governed and managed properly it can turn into a liability

4) Have accountability structures in place and create a culture that respects privacy

Framework for good privacy management



Board Governance

Set the broad direction of the organisation and ensure delivery of good governance of personal information and privacy through the setting of:

- Vision
- Values
- Board, Audit & Risk Committee oversight
- Assurance
- Accountability

Accountability

Defined and measurable through:

- Metrics
  - Client satisfaction
  - KPIs
- Monitoring
- Reporting

Leadership

Ensure efficient and effective delivery through:

- Organisational commitment
- Leadership and management structure
- Privacy strategy
- Culture
- Risk management

Privacy Programme

Develop and strengthen privacy management through:

- Defined roles and responsibilities
- Implementation of all the IPPs/HIPRs
- Privacy policies and procedures
- Privacy by Design
- Training and education
- Third party contracts and relationships
- Breach and incident management
- Complaints handling
- Review and Assess

User-centricity

- Respect for the individual:
  - □ Transparency
  - □ Usability
  - □ Control
  - □ Accountability
  - □ Data minimisation
  - □ Reduce trackability

- Examples:
  - □ Notifying collection – iPhone’s location arrow
  - □ Default settings – Google+

Privacy by Design

1. ***Proactive*** not Reactive;
Preventative not Remedial
2. Privacy as the ***Default Setting***
3. Privacy ***Embedded*** into Design
4. Full Functionality: ***Positive-Sum***, not Zero-Sum
5. End-to-End Security – ***Full Lifecycle Protection***
6. ***Visibility*** and ***Transparency*** – Keep it ***Open***
7. ***Respect*** for User Privacy – Keep it ***User-Centric***

PbD
www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept that I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

1. *Proactive* not Reactive; *Preventative* not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

Building trust and innovative privacy solutions

Privacy Impact Assessments

- Identify and manage privacy risks and opportunities
- Features of PIA:
  - Prospective – looking at the future privacy impacts
  - Iterative – conducting analysis and feeding back into the design process
  - Risk & opportunity management – for both org and individuals

INFORMATION
INTEGRITY
SOLUTIONS

Assurance and Review

- Monitor compliance with privacy and security policy
- Periodically review new risks and adequacy of existing measures
- Update policies and procedures when required

Building trust and innovative privacy solutions

Conclusion

- Data protection regulation increasing
- Privacy challenges
- Case study: ACC
- Framework for good privacy management

Further information

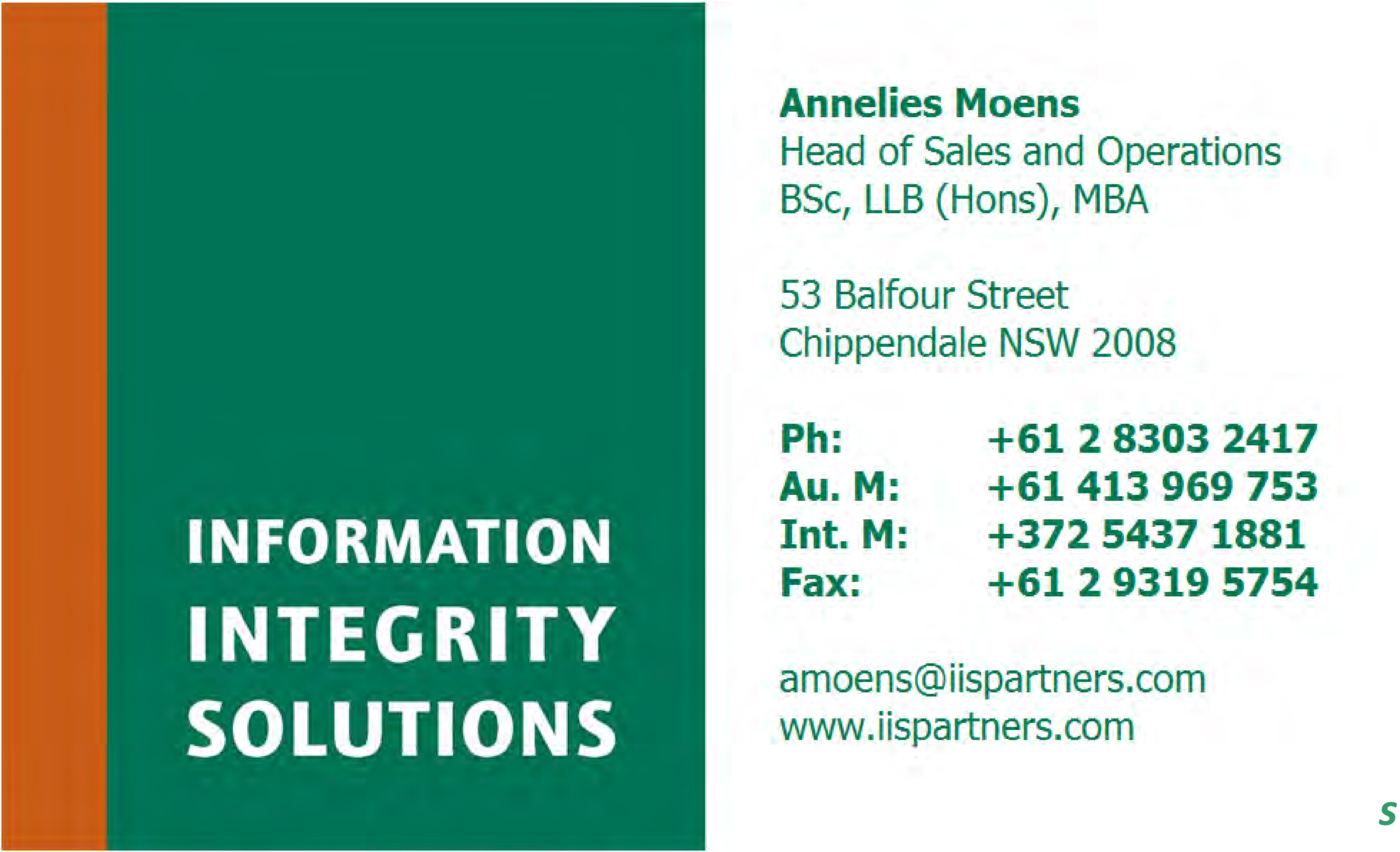
- Why Managing Customer Privacy Can Be An Opportunity, Avi Goldfarb and Catherine Tucker MIT Sloan Management Review Spring 2013, Vol.54 No.3
- Global Cloud Survey: the Implementation Challenge, KPMG, 2013 http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/cloud-computing/Documents/the-cloud-takes-shape.pdf
- Cloud Computing in 2013 - What legal commitments can you expect from your provider? Shelston IP, March 2013 http://www.shelstonip.com/case_study.asp?cid=13
- The Post Breach Boom, Ponemon Institute, February 2013 http://pages.soleranetworks.com/rs/soleranetworks/images/Ponemon%20Report-Post%20Breach%20Boom%202013.pdf
- New Zealand Cloud Computing Code of Practice, Institute of IT Professionals New Zealand, June 2012 http://www.nzcloudcode.org.nz/wp-content/uploads/2012/05/NZCloudCode.pdf
- 2012 Data Breach Investigations Report, Verizon, 2012 http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

INFORMATION INTEGRITY SOLUTIONS

Further information

- Rethinking Personal Data: Strengthening Trust, World Economic Forum, May 2012 http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf
- Privacy in the Cloud: Key Questions, by Annelies Moens, Australian Corporate Lawyers Association, March 2012 Vol 22, Issue 1
- Cloud Computing Contracts White Paper A Survey of Terms and Conditions, Truman Hoyle Lawyers, April 2011 http://www.itnews.com.au/pdf/Cloud-Computing-Contracts-White-Paper.pdf
- Privacy Impact Assessment Guide, Office of the Australian Information Commissioner, May 2010 http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.pdf
- Privacy By Design – 7 Foundational Principles, Ann Cavoukian http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

Questions?



INFORMATION
INTEGRITY
SOLUTIONS

Annelies Moens
Head of Sales and Operations
BSc, LLB (Hons), MBA

53 Balfour Street
Chippendale NSW 2008

Ph:	**+61 2 8303 2417**
Au. M:	**+61 413 969 753**
Int. M:	**+372 5437 1881**
Fax:	**+61 2 9319 5754**

amoens@iispartners.com
www.iispartners.com