INFORMATION
INTEGRITY
SOLUTIONS

legalwise
SEMINARS

Privacy, the Cloud and Data Breaches

Annelies Moens
Head of Sales and Operations,
Information Integrity Solutions

Legalwise Seminars
Sydney, 20 March 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

nib

CommonwealthBank

ANZ

CISCO

Westpac

Microsoft

Building trust and innovative privacy solutions

Overview

- Changing privacy regulation across the globe

- Cloud computing & privacy risks
- Safeguards
- Data breaches

INFORMATION INTEGRITY SOLUTIONS

Australia & New Zealand

Australia:

- Privacy Amendment (Enhancing Privacy Protection) Act 2012 received royal assent in December 2012
- Act to commence in March 2014 – 15 month implementation window

New Zealand:

- Law Commission recommends reform of Privacy Act and progress underway

INFORMATION
INTEGRITY
SOLUTIONS

Asia-Pacific

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

United States

- **Blueprint** for protecting consumer data privacy and promoting innovation in the digital economy
  - Consumer bill of rights
  - Multistakeholder process to develop Codes of Conduct
- FTC takes a more active role
  - Report: Protecting Consumer Privacy in an Era of Rapid Change
  - Increased enforcement activity to protect consumer privacy

Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT

FEDERAL TRADE COMMISSION | MARCH 2012

INFORMATION
INTEGRITY
SOLUTIONS

United States

Main action items for the FTC:

- Do-Not-Track
- Mobile services
- Data brokers
- Large platform providers

European Union

Draft Regulation for the protection of individuals and their personal data

- One law for the entire EU

Strengthened Consent	Extraterritorial application
Accountability of processors	Significant penalties
Mandatory privacy officers	The right 'to be forgotten'
Data breach notification	The right of 'portability'

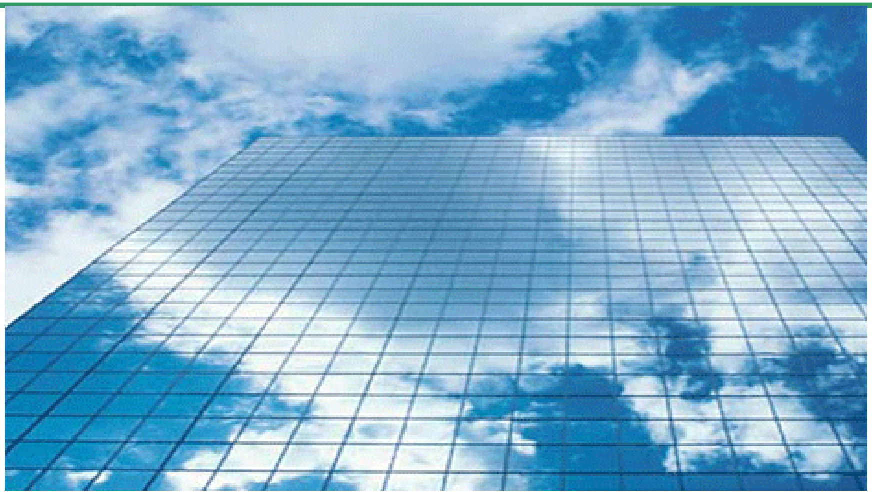
INFORMATION INTEGRITY SOLUTIONS

European Union

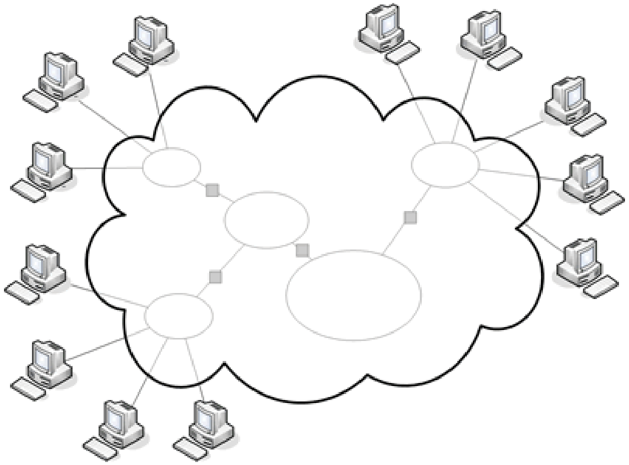
Progress on Regulation so far:

- Multiple interests – companies (especially American), civil liberties proponents, data protection officials in the EU member states
- Amendments proposed by parliamentary committee (the Albrecht draft) in Jan 2013
- Voting on final Regulation not expected until late 2013

Building trust and innovative privacy solutions



Cloud Computing



Building trust and innovative privacy solutions

What is cloud computing?

"[A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (eg, networks, servers, storage, applications and services)…"

National Institute of Standards and Technology (2011)

- On-demand service
- Resource pooling - scalable
- Measured service

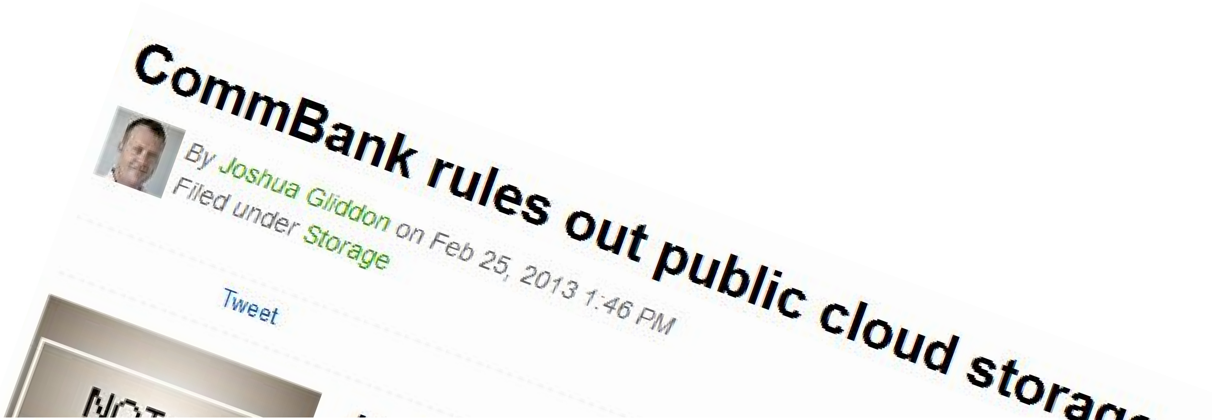
- Rapid elasticity
- Broad and remote network access

What is cloud computing?

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

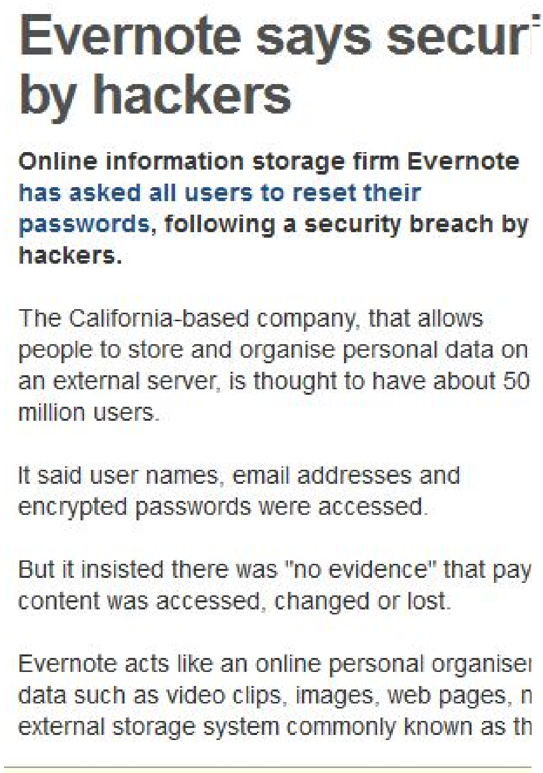
Why some orgs engage CSPs

- Connecting with multiple devices, business agility and cost-cutting were the top three reasons cited for adopting cloud services (TNS)
- 88% of Australian organisations saw improvement in their IT departments since adoption of cloud (TNS)
- Australian public cloud market to reach $3.2 billion this year (Gartner)



CommBank rules out public cloud storage

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



Evernote says securi by hackers

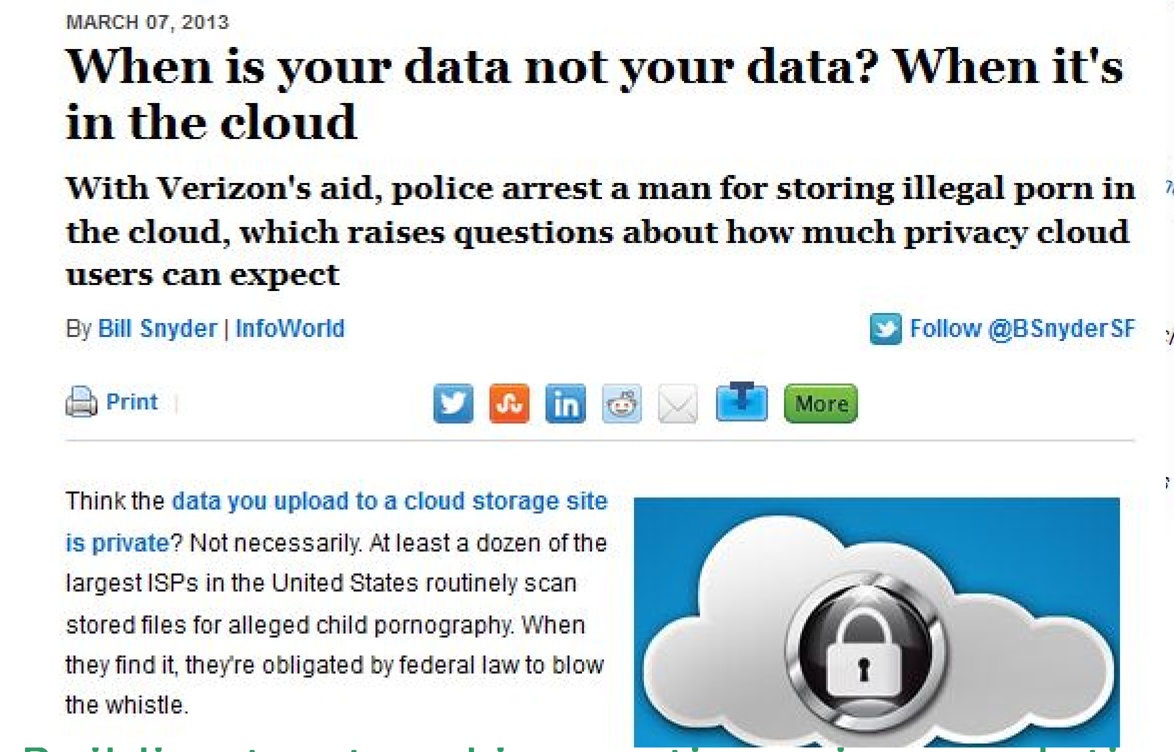
Online information storage firm Evernote has asked all users to reset their passwords, following a security breach by hackers.

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 organiser data such as video clips, images, web pages, n external storage system commonly known as th



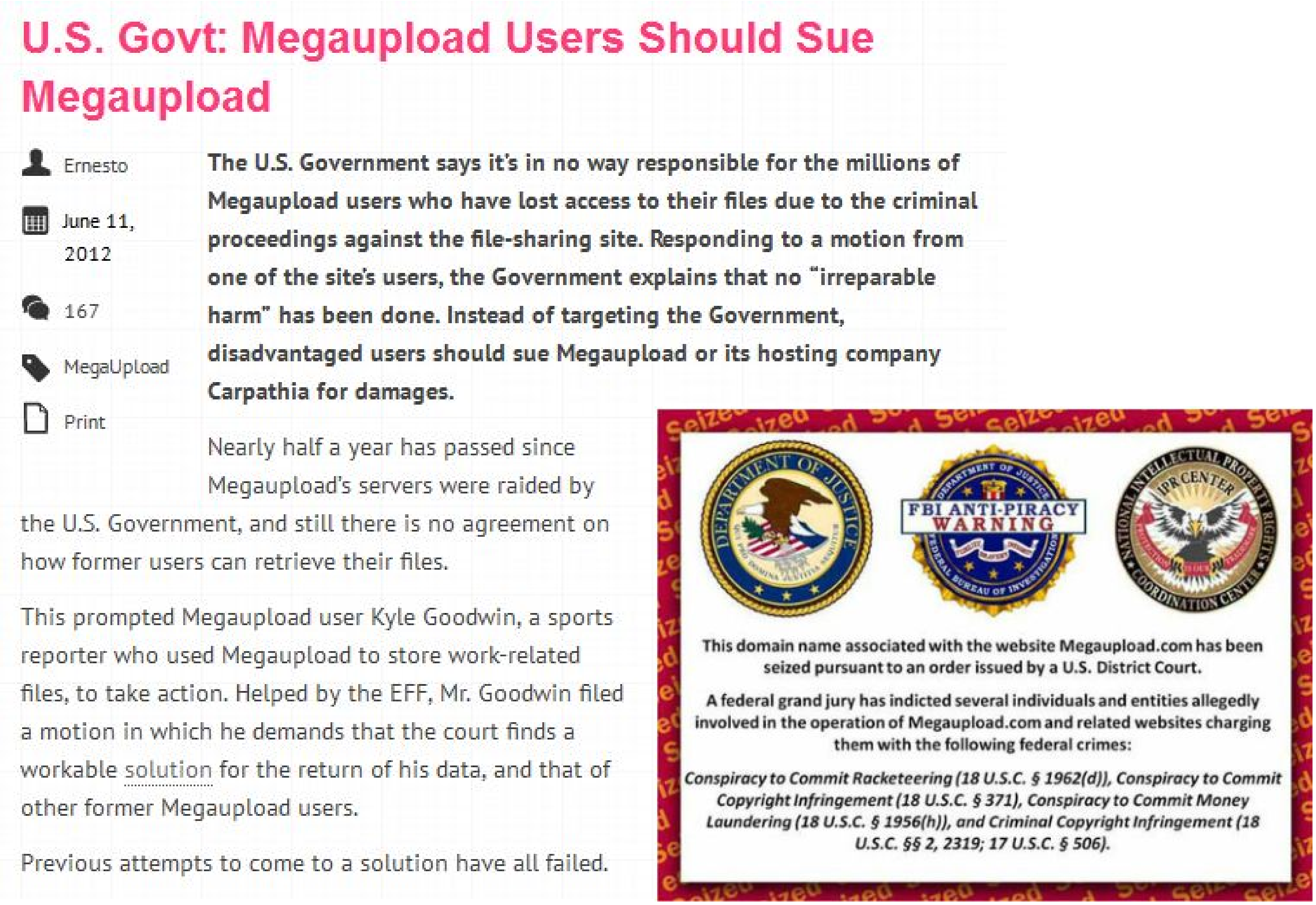
MARCH 07, 2013

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

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.

Seized
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?

What's in the contract?

Among existing contracts for cloud-based services in Australia, many have problematic provisions:

- Not addressing access to or deletion of data, on service termination or breach of contract
- Limitation of liability for direct damages, exclusion of liability for indirect damages
- Unilateral variation of terms and conditions

What's in the contract?

- Onus on the customer to ensure privacy rules are complied with
- Onus on the customer to take security measures, with no mention of what would happen in the event of a security breach
- No control over third parties who receive the personal information in the course of providing the service

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

APPs and Cloud

- APP 1: current and clear policy about management of personal information, including disclosures to overseas recipients and their location
- APP 5: notice when personal information is collected, including if disclosed to overseas recipients and their location
- APP 8 and section 16C: in some circumstances may be liable for breach of APP by overseas recipient
- APP 11: destroy or de-identify personal information

INFORMATION INTEGRITY SOLUTIONS

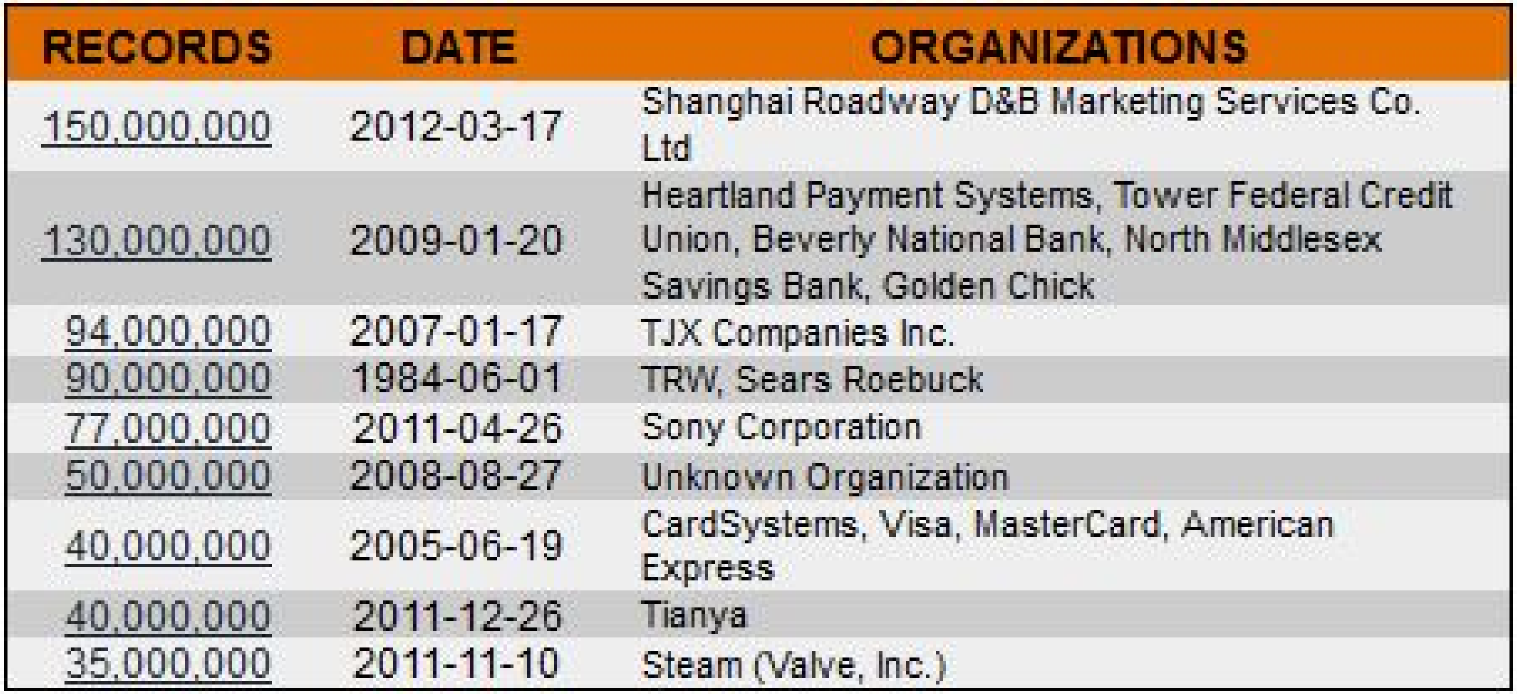
10 Safeguards

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. Don't put anything in the cloud that you wouldn't want a competitor or government to see
5. Clarify the rights of access, correction and deletion
6. Find out where and how the data will be kept
7. Find out the CSP's arrangements with subcontractors
8. Determine liability and accountability – what happens when things go wrong?
9. Have back-ups
10. Establish your own security measures

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
50,000,000	2008-08-27	Unknown Organization
40,000,000	2005-06-19	CardSystems, Visa, MasterCard, American Express
40,000,000	2011-12-26	Tianya
35,000,000	2011-11-10	Steam (Valve, Inc.)

Source: Largest Incidents: http://datalossdb.org/

INFORMATION
INTEGRITY
SOLUTIONS

Impact of a data breach

- The average total cost per data breach in Australian organisations rose to $2.16 million in 2011
- Having a data breach caused by a third party mistake cost on average 35% more per compromised record
- Malicious and criminal attacks are the main cause and are also the most expensive, at $183 per record
- Organisations with external consulting support reduced cost of data breach by up to $45 per record

(*2011 Cost of Data Breach Study: Australia, Ponemon Institute LLC (sponsor Symantec), March 2012*)

Causes of data breach

Malicious or criminal attack (36%)

- Hackers or criminal insiders (employees, contractors, cloud providers, business partners) typically cause the data breach
- Viruses, malware, worms, trojans
- SQL injection
- Theft of data-bearing devices
- Social engineering

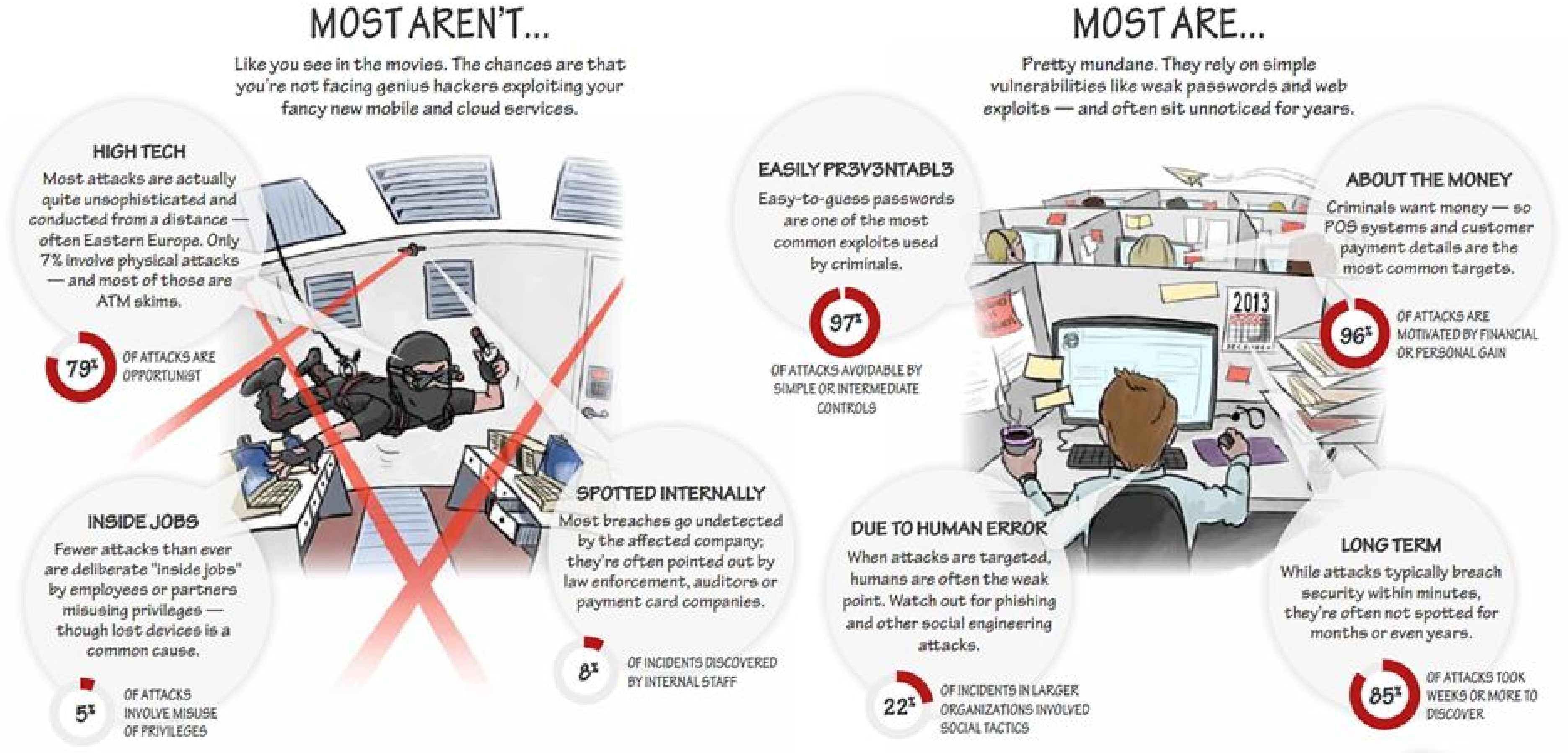
Negligence (32%)

- Negligent employee or contractor
- IT and business process failures

System glitch (32%)

(*Based on data breaches experienced by 22 Australian companies within 10 industry sectors in 2011 – Cost of Data Breach Study: Australia, Ponemon Institute LLC (sponsor Symantec), March 2012*)

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

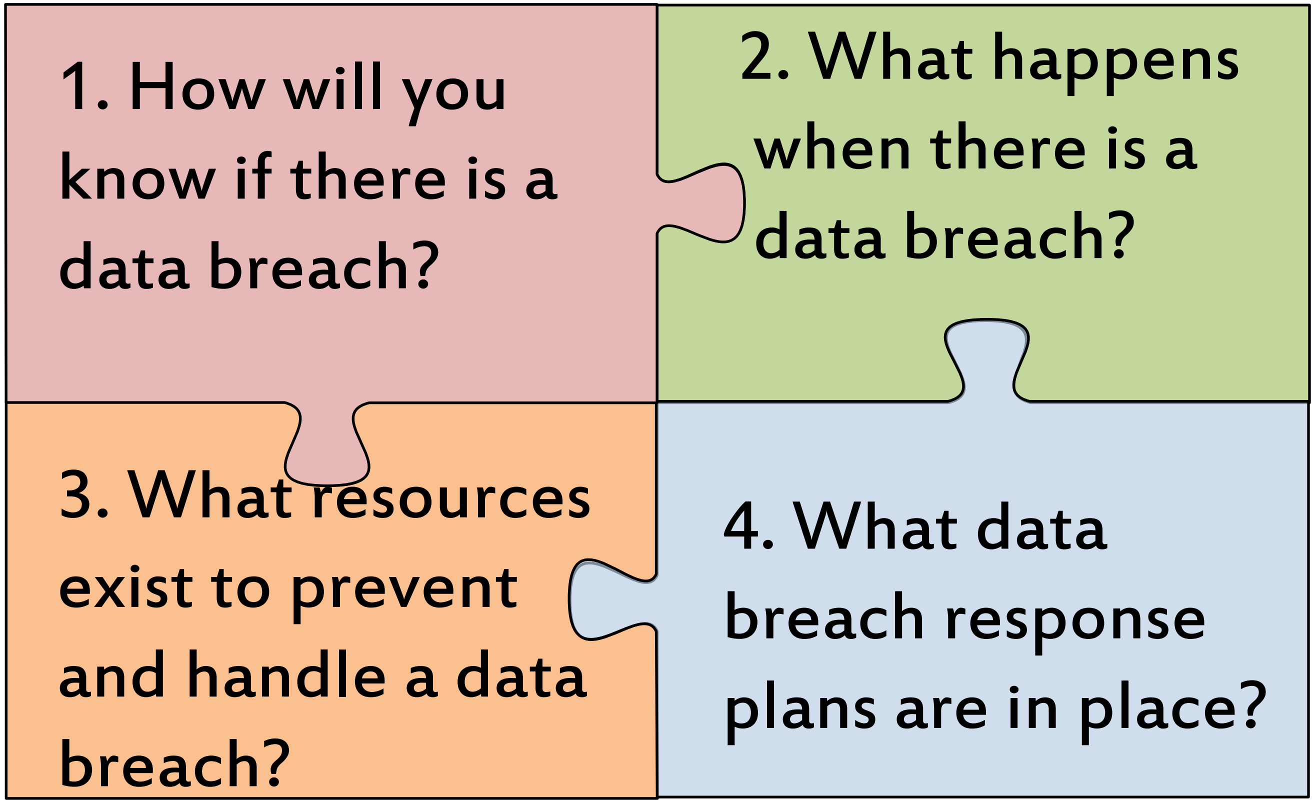
LONG TERM

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: Based on Verizon 2012 Data Breach Investigations Report

Data Breaches



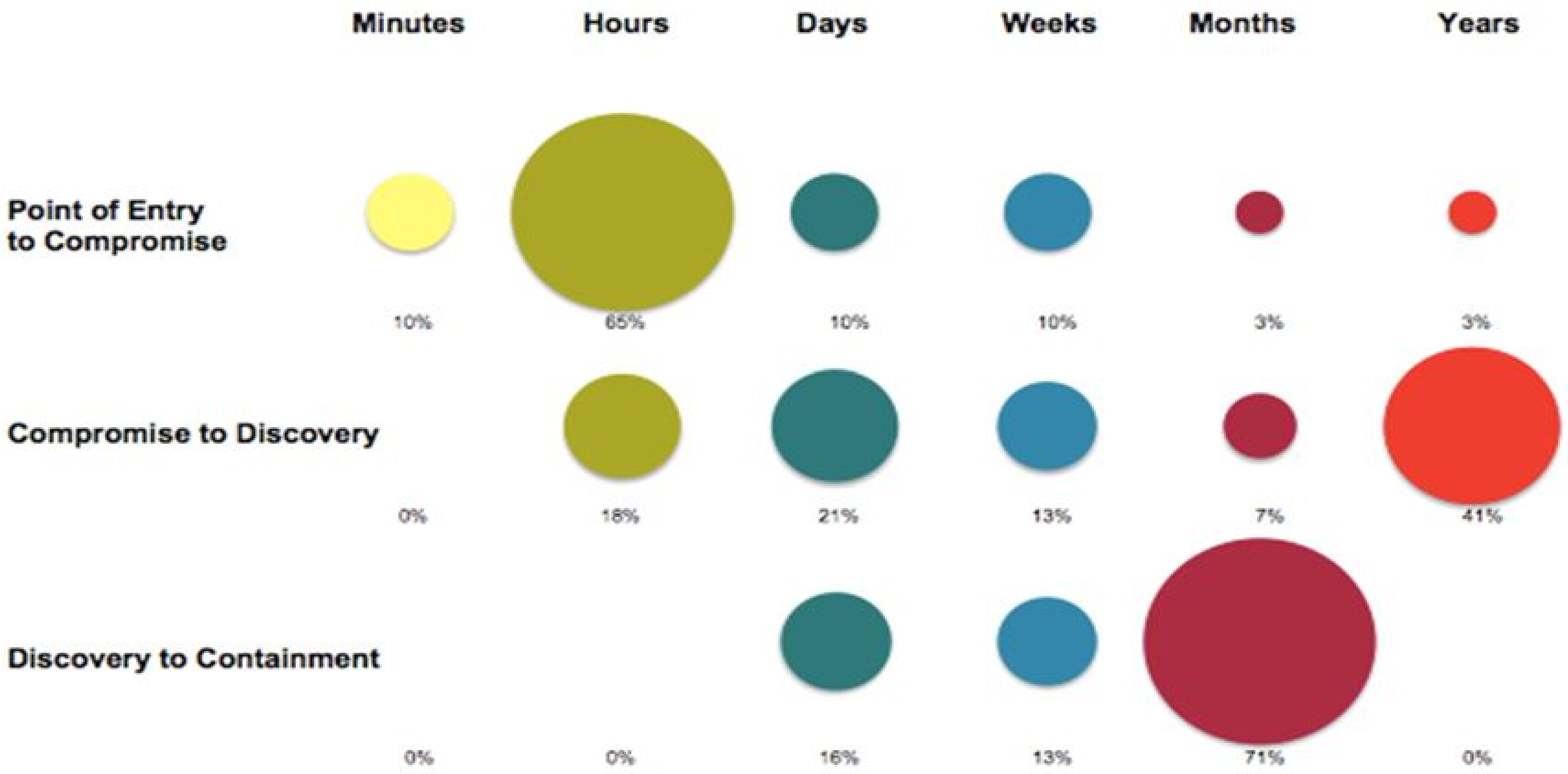
1. How will you know if there is a data breach?

2. What happens when there is a data breach?

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

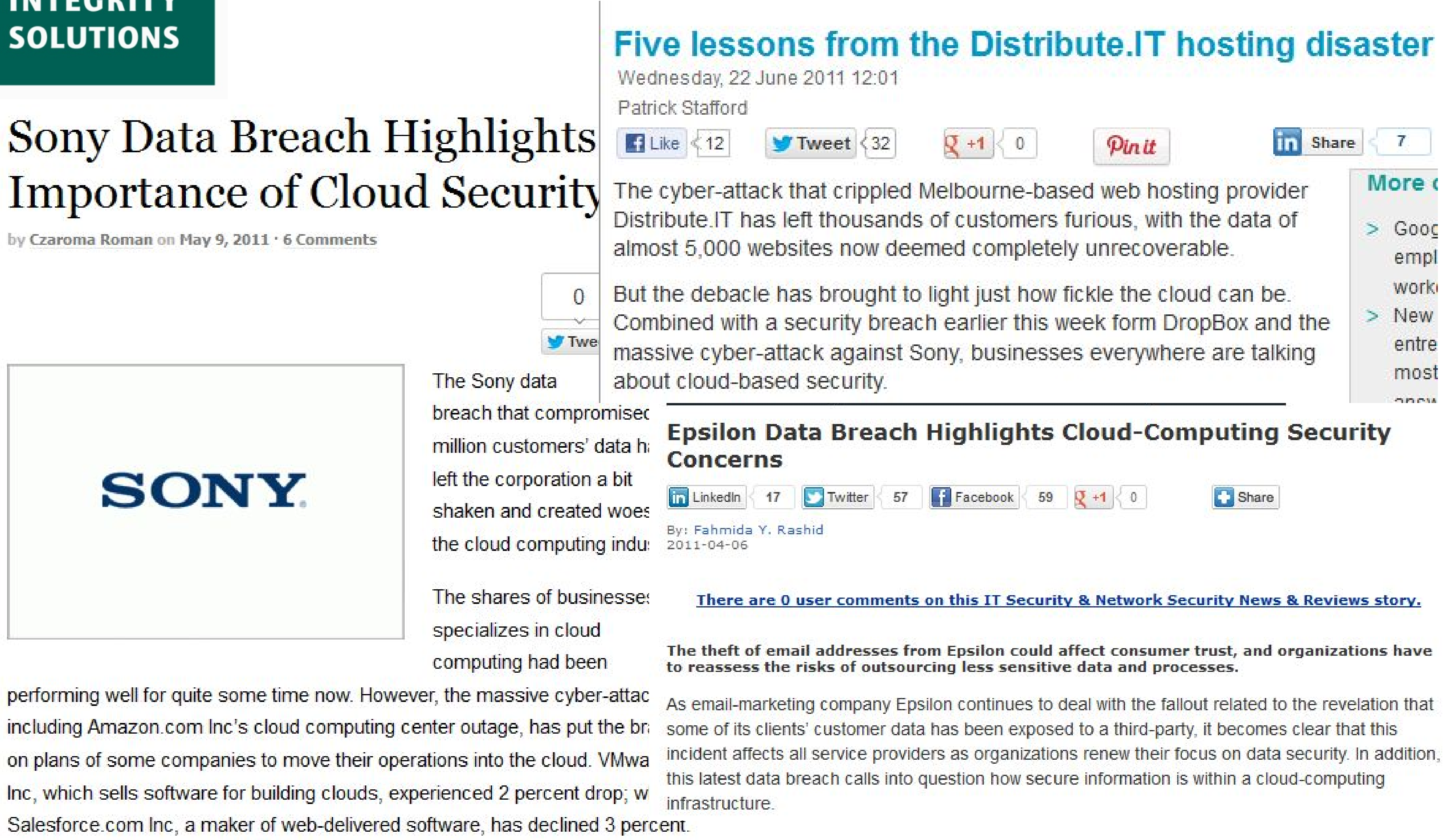
4. What data breach response plans are in place?

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



Reproduced with permission from Verizon: Based on Verizon 2012 Data Breach Investigations Report

2. What happens when there is a data breach?



Sony Data Breach Highlights Importance of Cloud Security

by Czaroma Roman on May 9, 2011 · 6 Comments

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

The shares of businesses 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 bra 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.

Epsilon Data Breach Highlights Cloud-Computing Security Concerns

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.

Building trust and innovative privacy solutions

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

Conclusion

- Data protection regulation increasing
- Privacy risks of cloud
- Safeguards
- Data breach is expensive
- How to respond to a data breach

INFORMATION
INTEGRITY
SOLUTIONS

Further Information

- 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

- Privacy and Cloud Computing for Australian Government Agencies, February 2013
  http://agimo.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf

- Draft Report on Cloud Service Provider Certification Requirements for the Australian Government, Department of Finance and Deregulation, December 2012
  http://agimo.gov.au/files/2012/12/csp-assurance-requirements-v0.5.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

- Data breach notification - A guide to handling personal information security breaches, Office of the Australian Information Commissioner, April 2012
  http://www.oaic.gov.au/publications/guidelines/privacy_guidance/Data_breach_notification_guide_April2012FINAL.pdf

- Privacy in the Cloud: Key Questions, by Annelies Moens, Australian Corporate Lawyers Association, March 2012 Vol 22, Issue 1

Building trust and innovative privacy solutions

Further Information

- 2011 Cost of Data Breach Study: Australia, Ponemon Institute LLC (sponsor Symantec), March 2012
  http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-australia-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_Australia
- 2012 Data Breach Investigations Report, Verizon, 2012
  http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
- 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 in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, Prepared by Robert Gellman for the World Privacy Forum, February 2009
  http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

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