Australian Government
Australian Institute of Criminology

Cambridge Symposium 2014

Workshop – The criminal use of online data

The nature and extent of criminal misuse of personal information

Dr Russell G Smith
Principal Criminologist

Outline

A note on terminology and concepts

- *Terms*: frauds, scams, tricks, cons, swindles, rooks, flim-flams, gyps
- Identity elements and identity misuse typologies

Survey research – prevalence

- UK – National Fraud Authority Identity Fraud Survey 2012
- USA – Bureau of Justice Statistics Survey – ID Theft Supplement 2012
- Aust – ABS Personal Fraud 2011; AIC Identity Crime & Misuse 2013

Survey research – how information is obtained and misused

- How personal information was obtained and misused (AIC survey)
- Personal information at risk of misuse (AIC survey)
- Verizon Data Breach Investigations Report 2014
- Anti-Phishing Working Group Report Q-1 2014

Using evidence to minimise risks

- Identifying high-risk activities and individuals
- Using information productively

A note on terminology and concepts

Identity elements (UK Cabinet Office)

- *Attributed identity*: attributes that are given to a person, usually at birth – name, gender, date and place of birth
- *Biometric identity*: unique attributes – iris, fingerprint, retina, DNA profile gait, dynamic signature, keystroke behaviour
- *Biographical identity*: attributes that build up over one's life – education, qualifications, employment, marriage, property registrations
- *Chosen identity*: attributes that are chosen by a person – pseudonyms, nicknames, usernames, passwords, avatar

Identity misuse typologies

- *Identity takeover*: taking on another person's identity without permission
- *Identity licensing*: allowing someone to make use of your identity
- *Identity exchange:* synthetic identity fabrication of two or more people
- *Identity creation*: creating a new identity not belonging to anyone else

Derived from: Bert-Jaap Koops (Tilburg University 2009)

Misuse of personal information in the UK

National Fraud Authority identity fraud survey 2012

- Nationally representative sample of 4,213 adults, 18 years and over
- Questions on prevalence and cost of identity fraud against individuals
- Excludes identity misuse in the public & private sectors and charities (18% of private sector and 14% of charities suffered identity fraud)

Findings

- *Lifetime prevalence*: 27% (19% of these before 2012)
- *Prior 12 months prevalence*: 8.8% of adult population (4.3m adults)
- 2.7 million people lost money; mean loss of £1,203 each
- National estimated total cost of £3.3 billion in 2012

Notes

- Direct losses to UK adults, excluding indirect and response costs
- Cost excludes funds recovered by victims (e.g. from banks)

Source: National Fraud Authority (2014: 14)

Misuse of personal information in the United States

Bureau of Justice Statistics Identity theft survey 2012

- Nationally representative sample of 69, 814, aged 16 years and over
- Questions on prevalence and response to identity theft
- Reference period January to June 2011 (surveyed Jan-June 2012)

Findings

- *Lifetime prevalence*: 14% (34.2 million people nationally)
- *Prior 12 months prevalence*: 6.7% of people aged 16 and over
- 68% had direct or indirect losses for the most recent incident
- Mean loss of US$1,769 each; median loss of US$300
- National estimated total cost of US$24.7 billion

How personal information obtained

- Only 32% knew how their personal information had been obtained
- 43% of these said it had been obtained in a purchase or transaction

Source: Harrell & Langton (2013)

Australian Government
Australian Institute of Criminology

Misuse of personal information in Australia

ABS Personal fraud survey 2011

- Survey of 26,405 households; one respondent aged 15 years and over
- Questions on prevalence and responses to scams & identity fraud

Findings for 2010-11

- Personal fraud in 12 months before 2010-11: 6.7% of Aust population
- Scams 2.9%, ID Fraud 4.0% (credit card fraud 3.7%; ID theft 0.3%)
- National estimated total cost of personal fraud A$1.4 billion

AIC Identity theft and misuse survey 2013

- 5,000 Australians aged 15 years and over in all states & territories
- 23 questions on nature and extent of misuse of personal information

Findings

- Lifetime prevalence: 21% (1,032 respondents)
- 12 months prevalence: 9.4% (460 respondents)
- 54.3% suffered out-of-pocket losses (250)
- Mean loss of A$4,101 each; median loss of A$247; Max A$310,000

Sources: ABS (2012); Smith & Hutchings (2014)

How personal information was obtained (AIC survey)

Ways of obtaining personal information	n	%
Hacking a computerised device	92	20.0
From an online banking transaction	90	19.5
By email	84	18.3
From a website (e.g. online shopping)	72	15.7
From an ATM / EFTPOS transaction	51	11.0
By telephone (excluding SMS)	48	10.5
Theft of mail	44	9.6
Data breach (information stolen from an organisation)	44	9.6
In a face-to-face meeting (e.g. job interview, door-to-door)	35	7.5
From a social media site (e.g. Facebook, Linked-in)	32	6.9
By text message (SMS)	29	6.4
Theft of a personal document or copy	13	2.8
Other / don’t know	116	25.4

How personal information was misused (AIC survey)

Misuse on the most serious occasion in the last 12 months	n	%
To obtain money from a bank account (excluding super)	163	35.4
To purchase something	150	32.5
To apply for a loan or to obtain credit	37	8.1
To file a fraudulent tax return	33	7.2
To obtain money from an investment (e.g. shares)	30	6.5
To apply for a job	30	6.4
To open a mobile phone account	29	6.4
To provide false information to police	24	5.3
To obtain superannuation monies	23	5.1
To apply for government benefits	19	4.1
To open an online account (e.g. Facebook, eBay)	14	3.2
To rent a property	11	2.3
Other / don't know	109	23.6

Personal information most at risk of misuse

Attributed / biometric	Biographical	Financial / Property	Chosen
Name (40%)	Address (25%)	Credit card details (52%)	Password (19%)
Date of birth (22%)	Driver's licence (10%)	Bank account no (31%)	Username (18%)
Gender (19%)	Tax numbers (7%)	Credit history	PIN (8%)
Place of birth (9%)	Passport details (5%)	Liabilities / debts	Email addresses
Signature (8%)	Health numbers (5%)	Property title numbers	Avatar
Fingerprint (2%)	Citizenship	Mortgage details	Social media ID
Parental names	Medical history	Shares HIN (2%)	Pseudonym
Ethnicity	Spouse details	Utility account details	Nickname
Facial image	Childrens' details	Vehicle numbers	
Retinal-iris image	Marital status	ICT serial numbers	
DNA	Phone numbers		
Voiceprint			

Sources: Smith & Hutchings (2014); Canadian

United States Consumer Sentinel Network

Federal Trade Commission Report 2014

- Consumer complaints in the USA, January-December 2013
- 35% increase in identity theft complaints from 2003 to 2013

Findings

- 14% of the 2 million complaints concerned identity theft (290,056)
- 34% of ID theft concerned government documents or benefits fraud
- 17% of ID theft concerned credit card fraud
- 14% of ID theft concerned phone and utilities fraud
- 8% bank fraud; 6% employment fraud; 4% loan fraud

Country location of companies with complaints

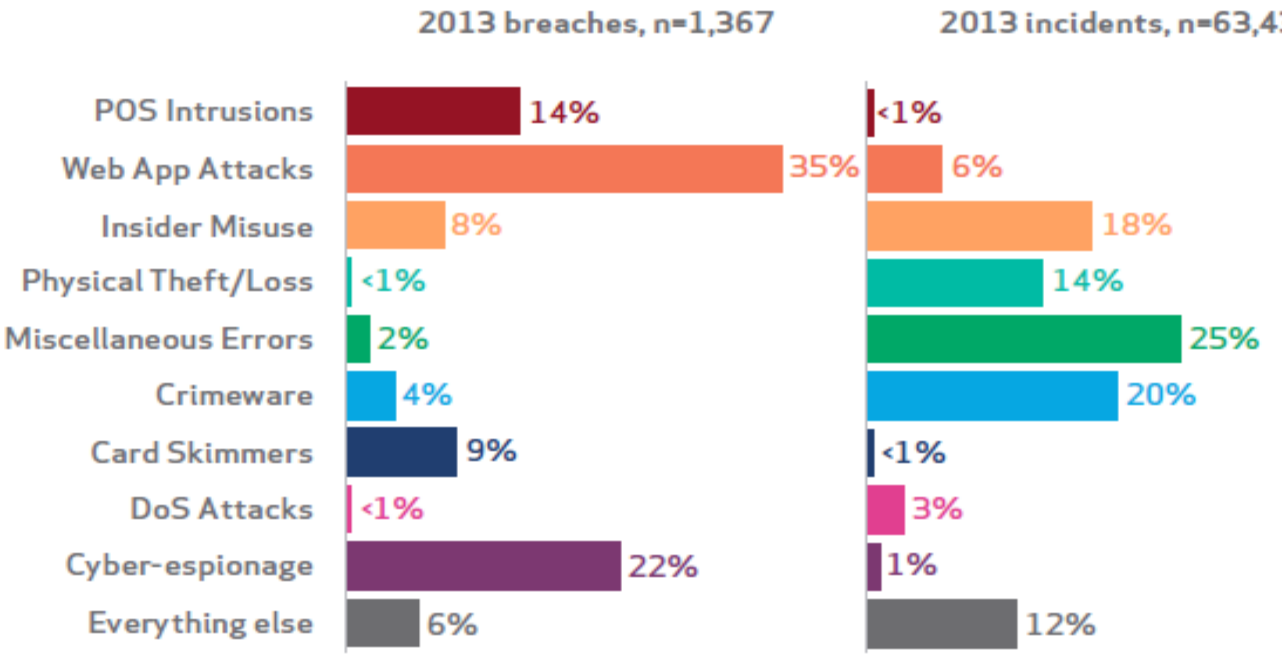
- 88% – United States; 4% Canada
- 1% – UK, Nigeria, India, China
- < 1% – Jamaica; Mexico; Philippines; Ghana

Source: Federal Trade Commission (2014)

International data breaches

Verizon Data Breach Investigations Report 2014

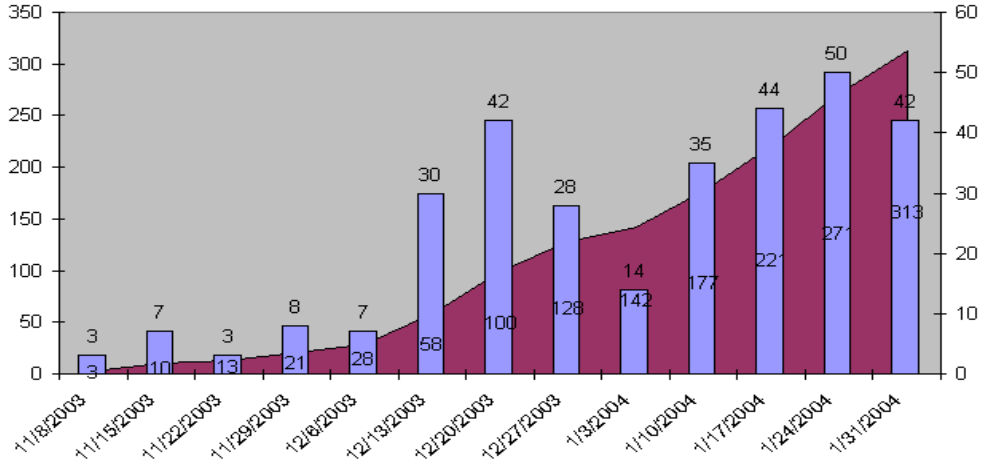
- Study of data breaches affecting organisations in 95 countries
- *Incident*: A security event that compromised the integrity, confidentiality or availability of an information asset
- *Breach*: Incidents resulting in disclosure or potential exposure of data



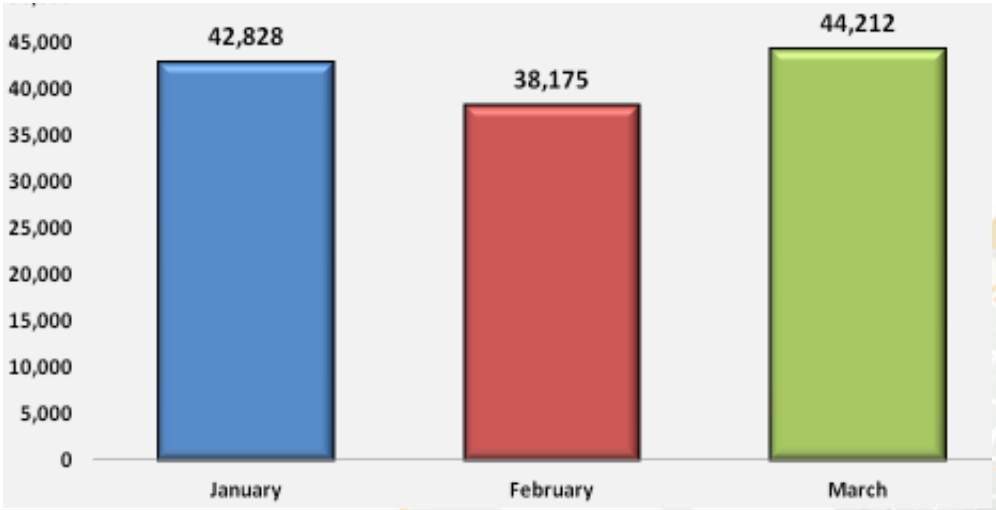
Source: Verizon (2014: 14)

Obtaining personal information by phishing (APWG)

January 2004
- 176 unique attacks



January 2014
- 42,828 unique attacks



24,000% increase over 10 years

Source: http://www.antiphishing.org/phishReportsArchive.html

Using the evidence to minimise risks

Identifying high-risk activities

- Using insecure electronic technologies
- Failing to undertake verification of personal information

Identifying high-risk individuals

AIC Survey of 9,241 Victorians who had transferred funds to Nigeria using Western Union from 1 April 2007 to 31 March 2008 (12 months)

- *Demographics*: low income, poor education, unemployed, older age
- *Lifestyle*: depression, financial crises, job loss, serious illnesses
- *Risk taking*: trusting of strangers, impulsive – unable to wait for things

Using information productively

- *Targeted information to*: lower income groups, less educated, unemployed, older age groups, those with mental health problems or serious illnesses, those likely to be risk-takers
- *Target hardening ICT*: making high-risk behaviour impossible; forced training of users; real-time monitoring and notification of data breaches

Source: Ross & Smith (2011)

Australian Government
Australian Institute of Criminology

Russell.Smith@aic.gov.au