



Data Loss Prevention

Keeping our sensitive data out of the
wrong hands

Introduction.



Will Dougherty

will.h.dougherty@nz.pwc.com



Graeme McLellan

graeme.x.mclellan@nz.pwc.com

Overview & Agenda

1. **The Value of Information**
 - **To individuals**
 - **To organisations**
2. **Concept of Information Leakage**
 - **What is Information Leakage?**
3. **How is information leaked?**
 - **Examples**
4. **What can we do about it?**
 - **Preventative measures**
 - **Top 10 messages for your organisation**
 - **UK Personal Information Promise**
5. **Questions?**



The Value of Information

The Value of Information – to Individuals

- Leaked information could lead to private information becoming known by inappropriate persons, which could lead to
 - Loss of privacy
 - Identity theft
 - Financial impact
 - Security of residence

The Value of Information – to Organisations

- Intellectual Property
- Customer details
- Customer and supplier trust / confidentiality
- Embarrassment from negative publicity

The Value of Information – Real \$\$\$

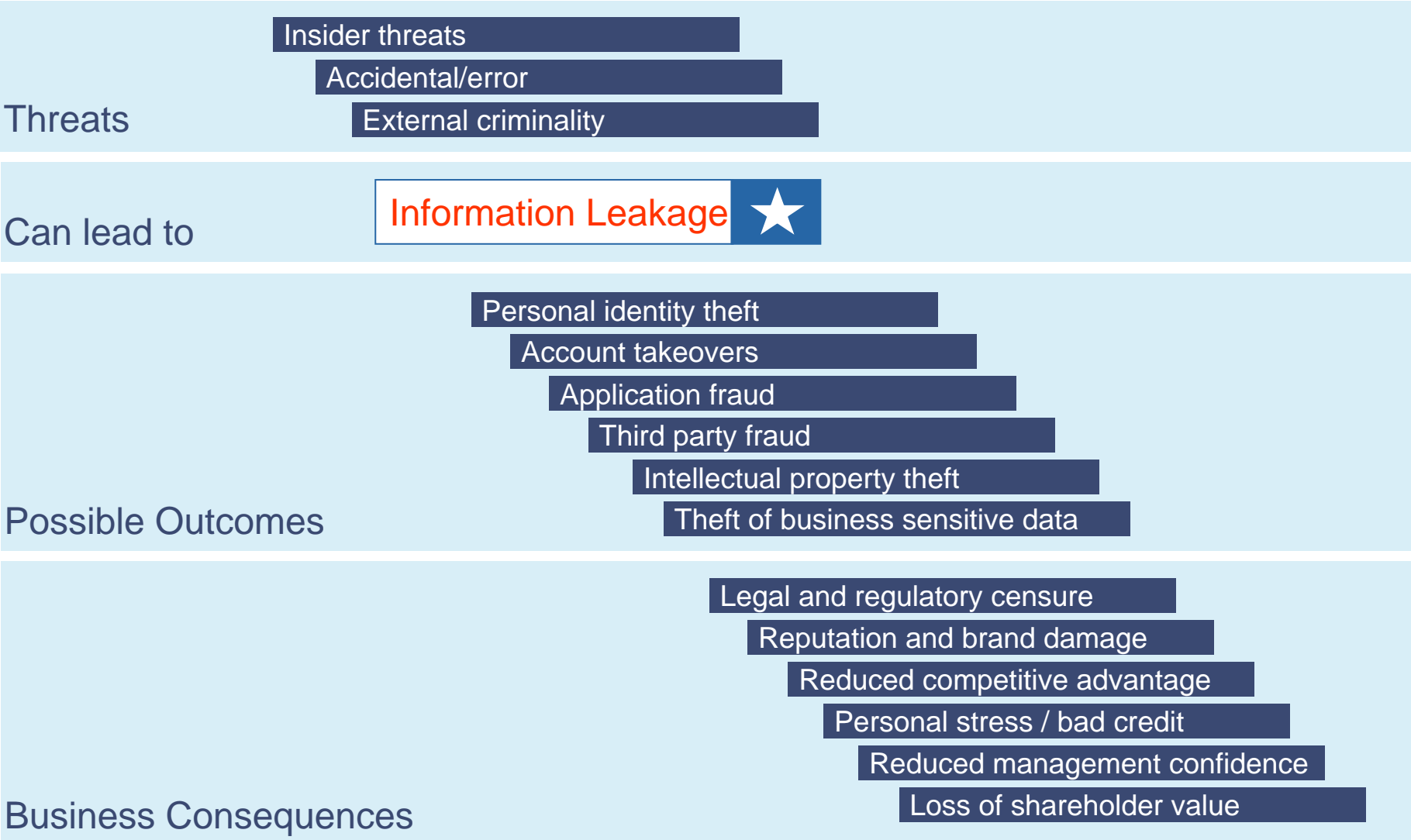
- Symantec noted in 2008 the asking prices for:
 - Stolen card data: US\$ 0.06 - 30
 - Bank accounts: US\$ 10 - 1000
 - Email accounts: US\$ 0.10 – 100
 - Full identities: US\$ 0.70 – 60

Source: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf



Concept of Information Leakage

Information Leakage - *problem on a page*



It's an information issue – top 5 fallacies

Top 5 fallacies - description

Customer data held was too limited or too piecemeal to be of value to fraudsters

Only high net worth individuals are attractive targets for identity fraudsters

Only large firms with hundreds of thousands of customers are likely to be targeted

The threat to data security is external – from burglars or computer hackers for example

Impervious to data breaches because no customer has ever alerted them to identity theft and fraud.





How is information leaked

Her Majesty's Revenue & Customs

loss of Child Benefit information



BBC News – 22 November 2007

PricewaterhouseCoopers

Page 12
May 2009

Further details on

Her Majesty's Revenue & Customs incident

The issue:

- National Audit Office information request October 2007
- Complete (not sanitised) data set sent by internal post (TNT)
- CD#1 not received, CD#2 sent -> both lost !

Why did this happen?

- NAO assumed authority; precedence set in prior audit
- Lack of data and process governance (entirely avoidable)
- Insecure methods of data storage and transfer
- Security not a management priority

Recommendations:

- PwC appointed by Chancellor of Exchequer
 - investigation & wider review
- HMRC have made progress on all major findings

Real Life New Zealand Examples

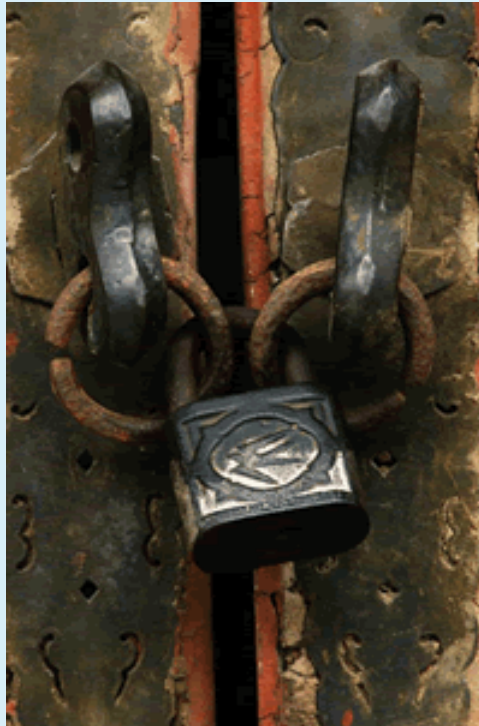
- Courier company **delivers** loan application pack to bank customer's neighbour.
- "Mental Health Inpatient Unit" **stamp** on envelope identified woman's health condition to flat mates.
- Housing NZ **documents** mistakenly sent out with eviction notices, revealing the address of a senior manager to gang members and forcing her to leave her home under police protection.
- Lack of **website security** provides details of all Mt Ruapehu ski-field 18,000 pass holders.

Real Life New Zealand Examples

- A sensitive police **manual** left with Mongrel Mob members during a raid.
- A police **camera** containing hundreds of evidence photos such as crash scenes, burglaries and battered women, left at a house.
- 5,900 Shell fuel card customer details exposed on **website**
- Over 900 Ticketek customers names and contact details **emailed** in error as an attachment.

Real Life New Zealand Examples

- Massey University's **intranet** exposed thousands of students' personal details including IRD numbers, exam results, addresses and phone numbers.
- Whangarei man walked out of an Oklahoma second-hand shop clutching an **MP3 player** with confidential US military files.



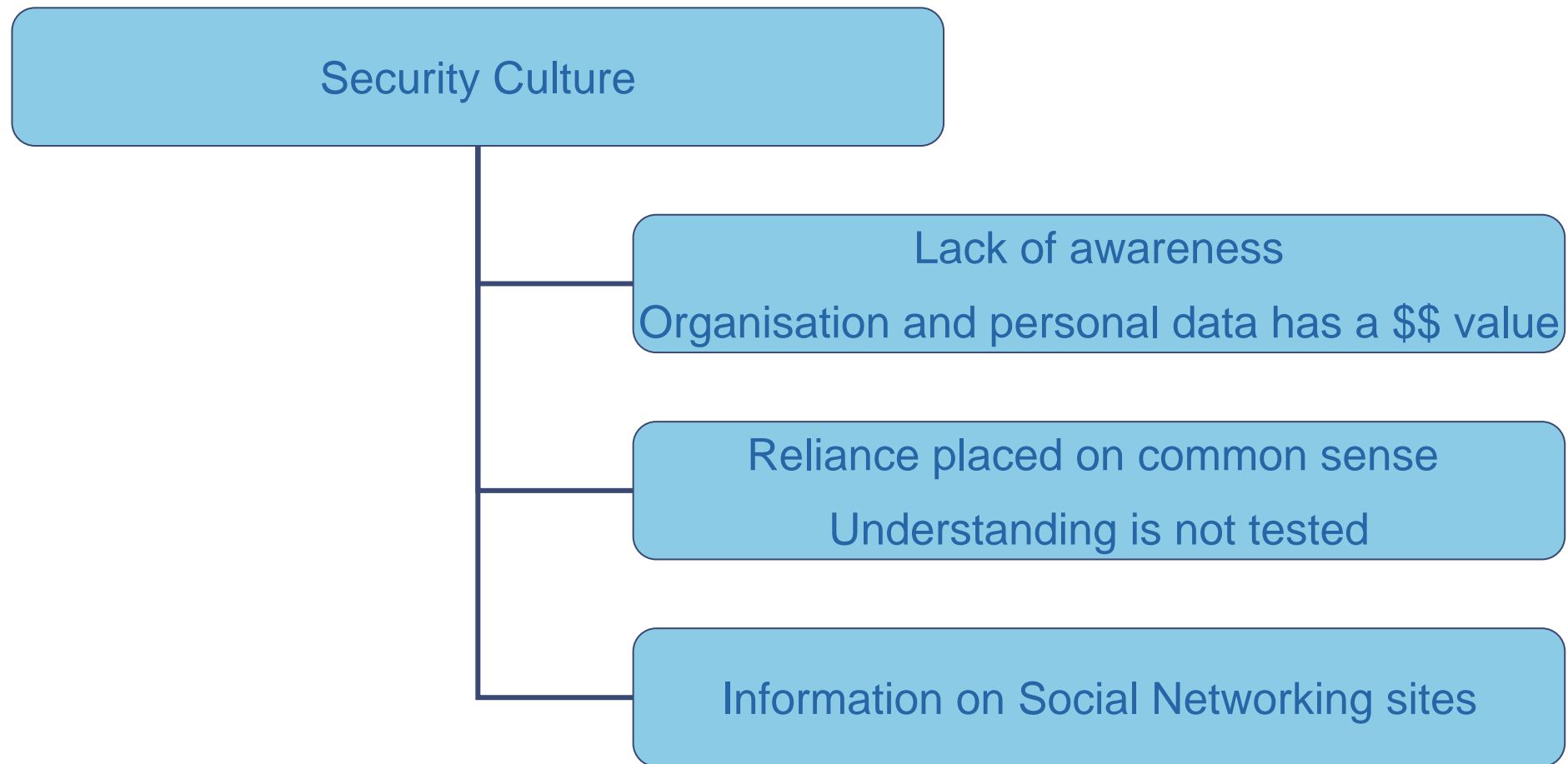
What can we do about it?

Preventative measures – what can businesses do?

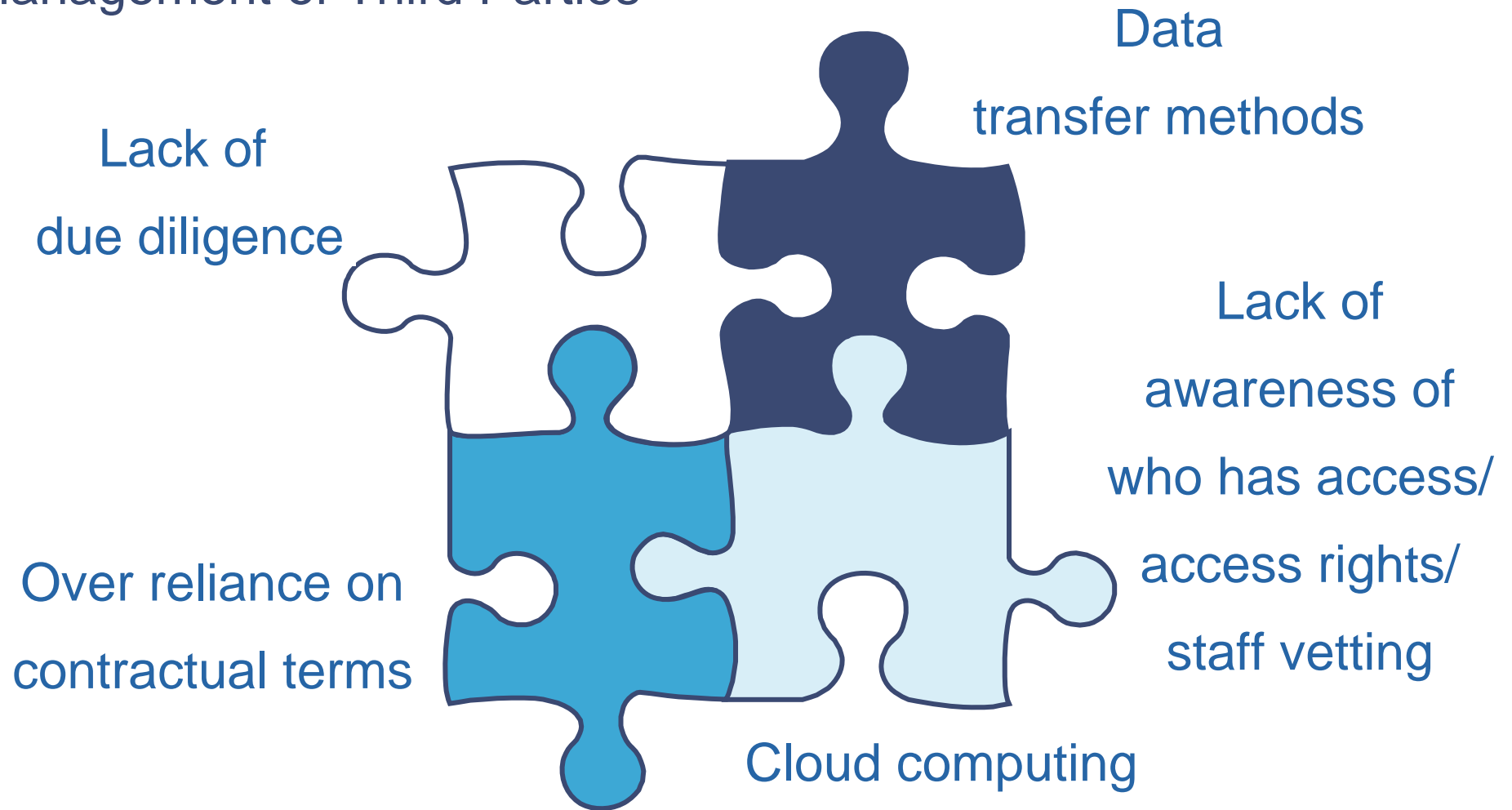
GOVERNANCE



Training & Awareness – do we have a security policy?!



Management of Third Parties



Top 10 key messages – checklist for your organisation

Governance

- Integrated security framework and governance **across** people, physical and IT
- Regular monitoring and compliance of adherence to policies
- Formalise risk management processes

Policies

- Simple, easily digestible security policies
- 3 step test for bulk transfers
 - Confirm the need to send, appropriate approval, enforce appropriate security
- Document management system - enables easier classification of data

People

- Culture (via awareness and training)
 - Staff satisfaction and morale can lead to increased due care and attention
 - Increase staff understanding of personal and business impacts

Data

- Tighter controls over 'hot spots' e.g. alerts over high net worth transactions or sensitive data
- Mandate hard-disk encrypted laptops and USB drives
- Robust disposal and destruction of documents and hardware

UK Personal Information Promise

Are you prepared to make a promise?

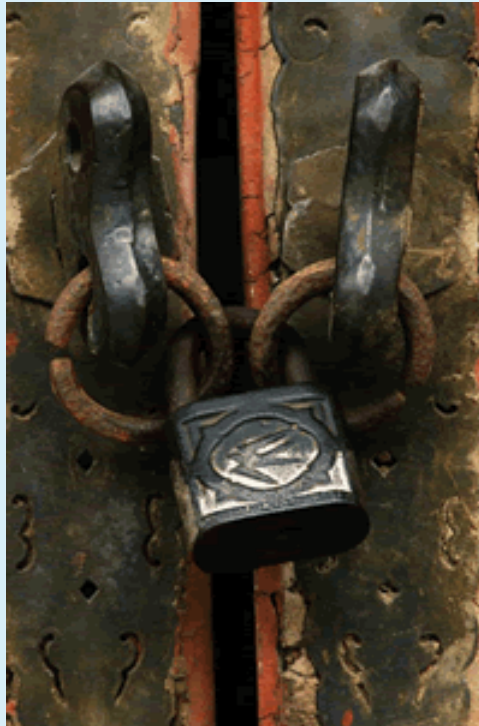
Introducing...



Sponsored by: *PRICEWATERHOUSECOOPERS* 

For further info, contact:
Sandra.Kelman@bp.com
(04) 903 3634

<http://www.iappanz.org>



Questions?