Directors Briefing: Privacy Governance: Risk and Opportunity for Directors

Wednesday 25 June 2014

Proudly Sponsored by:

AUSTRALIAN INSTITUTE
of COMPANY DIRECTORS

Privacy Governance

Malcolm Crompton FAICD

Managing Director

Information Integrity Solutions

INFORMATION
INTEGRITY
SOLUTIONS

The macro picture

INFORMATION INTEGRITY SOLUTIONS

Data as an asset

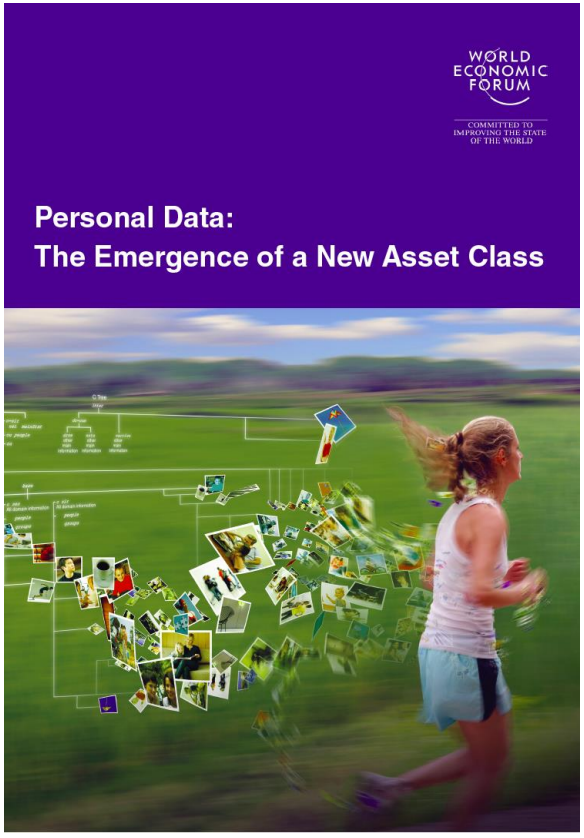
"Some day, on the corporate balance sheet, there will be an entry that reads, 'information'; for in most cases, the information is more valuable than the hardware that processes it."

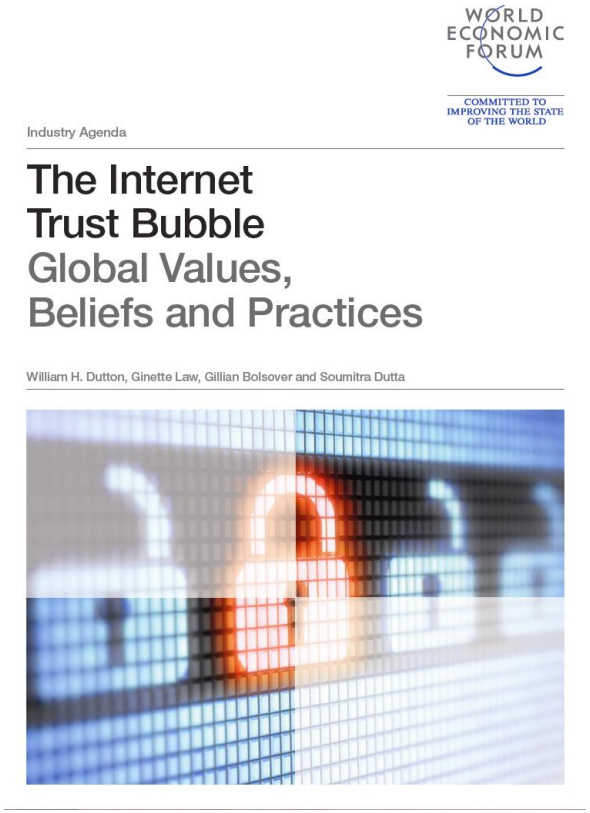
Rear Admiral Grace Murray Hopper

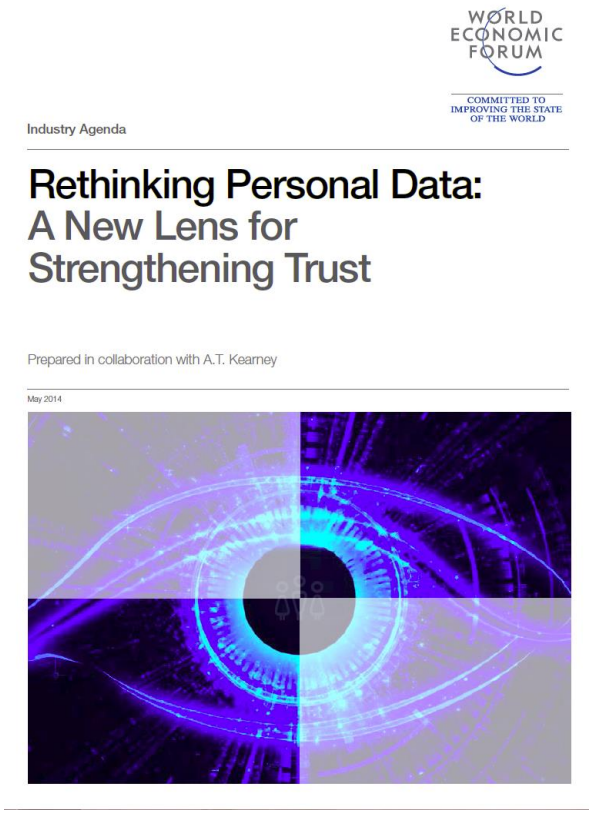
(American Computer programmer and Inventor of COBOL, 1906-1992)

INFORMATION INTEGRITY SOLUTIONS

Bringing up the rear







World Economic Forum Reports: www.weforum.org/issues/rethinking-personal-data

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

The micro picture: Changes to the Privacy Act

INFORMATION INTEGRITY SOLUTIONS

More focus on management of personal information

- **APP 1.2 – Open and transparent management of personal information**

> 1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:
>
> (a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

- "The bedrock principle"
- Read in conjunction with increased powers of the Privacy Commissioner

INFORMATION INTEGRITY SOLUTIONS

More focus on transparency and accountability

- **APP 1.3 – Privacy Policy**
  - Clearly expressed
  - Up-to-date
  - Mention any overseas disclosures
- **APP 7 – Direct marketing**
  - Tell people source of direct marketing info if asked
- **APP 8 – Accountability for cross-border disclosures**

INFORMATION INTEGRITY SOLUTIONS

Cross border accountability

- APP 8.1 obliges APP entities to take reasonable steps to ensure that the overseas recipient does not breach the APPs
  - In combination with section 16C, introduces **accountability**
- Two relevant exceptions in APP 8.2:
  - The overseas recipient is subject to a law or binding scheme that is substantially similar to the APPs with accessible enforcement mechanisms
  - The individual gives informed consent

INFORMATION INTEGRITY SOLUTIONS

Significant bolster of PC powers

- Conduct assessments of privacy compliance for both Commonwealth agencies and private businesses
- Request, develop, approve and register binding codes of practice relating to information privacy or credit reporting
- Accept and enforce written undertakings
- Conduct own motion investigations and take action, including:
  - Order the entity to take specified steps to ensure that a breach will not be repeated (e.g, independent privacy audits)
  - Order the entity to redress loss or damage suffered by individuals
- Impose fines of up to $1.7 million for entities that engage in serious and repeated interferences with privacy

INFORMATION INTEGRITY SOLUTIONS

How to respond:
It starts from the top!

INFORMATION INTEGRITY SOLUTIONS

Key ingredients

- Clear understanding of the value of personal information to the organisation
- Commitment from the Board
- Good data and privacy governance – structured oversight and accountability - dedicated staff if needed

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

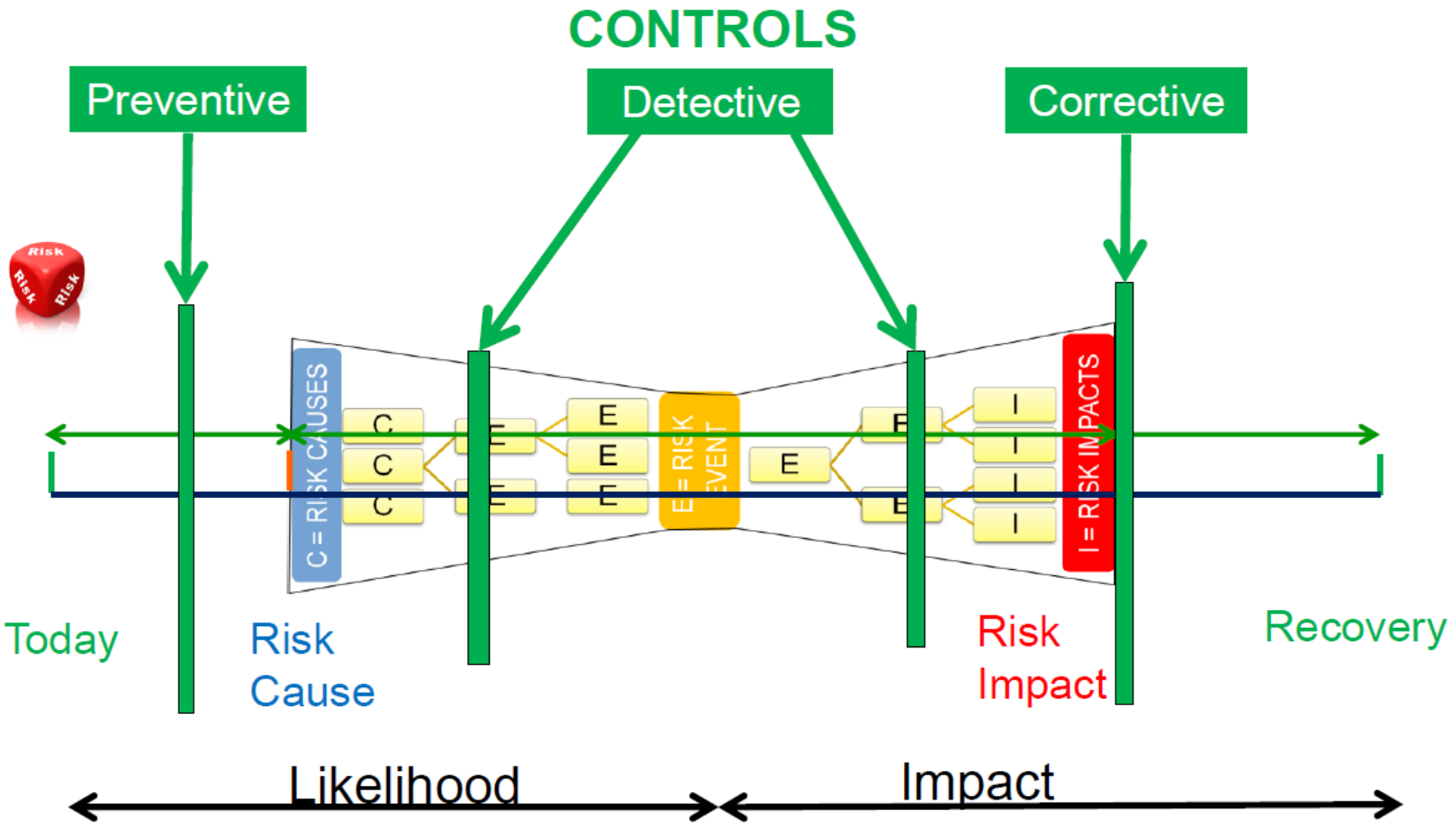
The five "must haves" for information management strategy

1. A senior role with management responsibility and accountability for privacy and information handling
2. A comprehensive internal privacy policy that reflects the operations of the entity, including a privacy by design approach
3. An appropriate weighting for privacy and the management of personal information in the entity's overall risk management framework
4. A privacy audit program to ensure staff comply with the entity's privacy policies and legislation
5. A data breach management plan that includes when individuals will be notified of breaches affecting them

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Framework for risk management



Source: David Tattam, Protecht (2013)

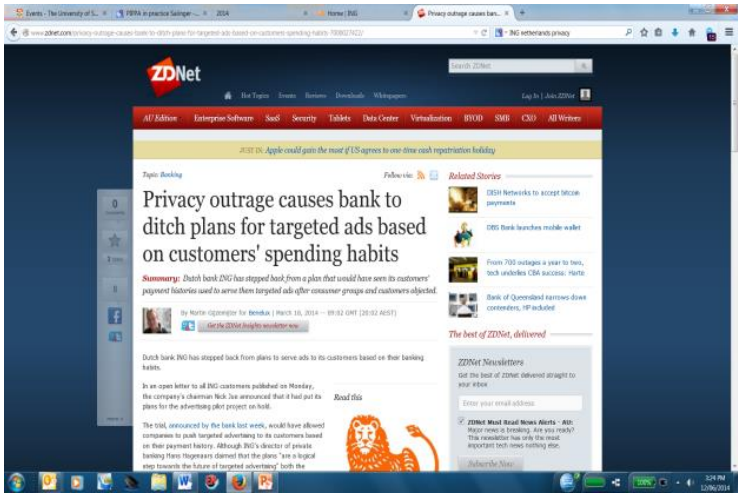
Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

A practical example of pitfalls Netherlands

ING DIRECT
Spend your life well

- Launched pilot using customer spending patterns to enable companies to offer discounts
- Public outcry on social media
- Government and Privacy Commissioner asking questions
- Pilot shelved and extensive explanation required



http://www.zdnet.com/privacy-outrage-causes-bank-to-ditch-plans-for-targeted-ads-based-on-customers-spending-habits-7000027422/

http://www.nltimes.nl/2014/03/10/ing-data-sharing-angers-mps-consumers/

http://www.ing.com/About-us/ING-and-the-use-of-customer-data.htm

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Helpful prevention and planning tools

- Organisation-wide – **Privacy Health Check**
- Before a change to handling of personal information (eg, policy, project, etc) – **Privacy Impact Assessment**
- **Privacy by Design** principles

PbD
www.privacybydesign.ca

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

The top 10 questions to ensure compliance

1. Do you have practices, procedures and systems to ensure compliance with the APPs and to handle inquiries or complaints?
2. Do you make your policies and practices relating to the handling of personal information available to customers in an easy to read format?
3. Do you limit the personal information you collect (collection limitation)?
4. Do you provide clear and easy to read privacy notice at the time or before you collect personal information?
5. Do you gain customer consent (or rely on an applicable exemption) if you use or disclose personal information for a purpose other than the primary purpose for which the information was collected?

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

The top 10 questions to ensure compliance cont'd

6. Do you give individuals a chance to opt-out of receiving direct marketing material?
7. If you disclose information overseas, have you taken the necessary steps to protect it from privacy breaches?
8. Have you implemented controls to ensure the personal information you hold and disclose is accurate, complete and up-to-date?
9. Are your security safeguards for protecting personal information appropriate for the sensitivity level of the information?
10. Do you have well-developed processes for customers to gain access and seek corrections to their own personal information

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

What now?

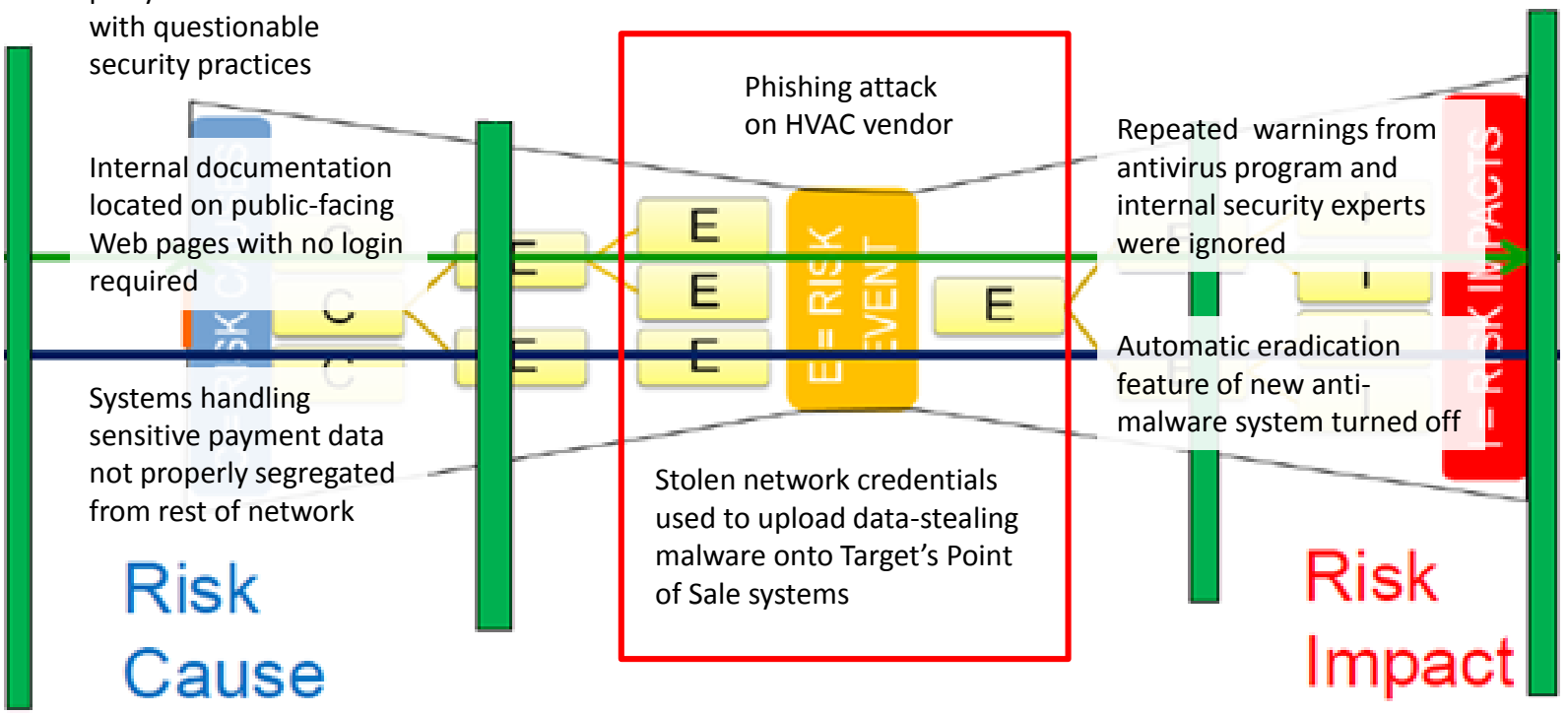
1. Engage your board and top executives
   - Strategic intent, not ad hoc tactics
   - Information management strategy
2. Consider the risk bow-tie when allocating resources (prevent/detect/correct)
3. Leverage planning tools into existing processes, eg
   - Privacy Health Check
   - PIA
   - Privacy by Design
   - Data Breach Response Plan

AND ABOVE ALL:

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Risk bow-tie in practice: Target data breach



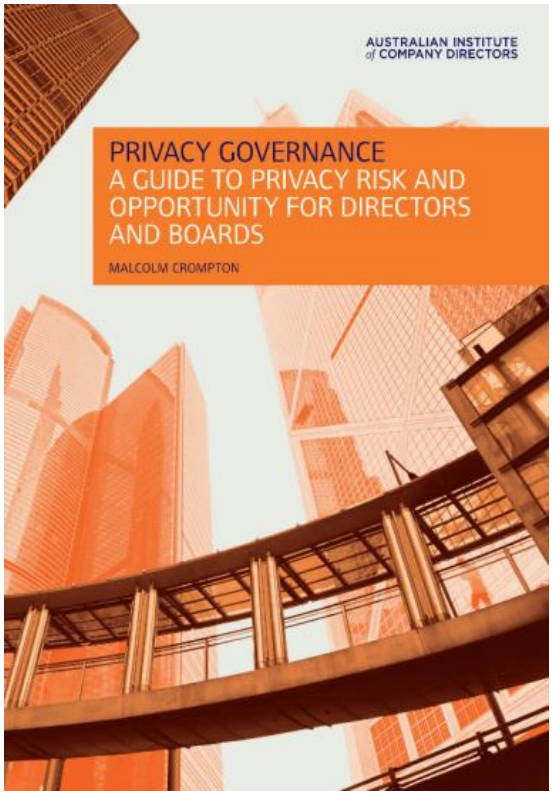
Source: David Tattam, Protecht (2013)

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

More help for Directors and Senior managers

- A Guide to Privacy Risk and Opportunity for Directors and Boards (2014)



http://www.companydirectors.com.au/Director-Resource-Centre/Publications/Book-Store/Privacy-Governance

Building trust and innovative privacy solutions

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: thought leadership; privacy notices and policies, Privacy by Design, Privacy Impact Assessments, governance and strategy, privacy health check, advisory services, data breach and crisis handling...

Australian Government

ACC PREVENTION. CARE. RECOVERY.

Microsoft

CommonwealthBank

APEC

CISCO

NBNCo Limited

Google Singapore

Building trust and innovative privacy solutions