



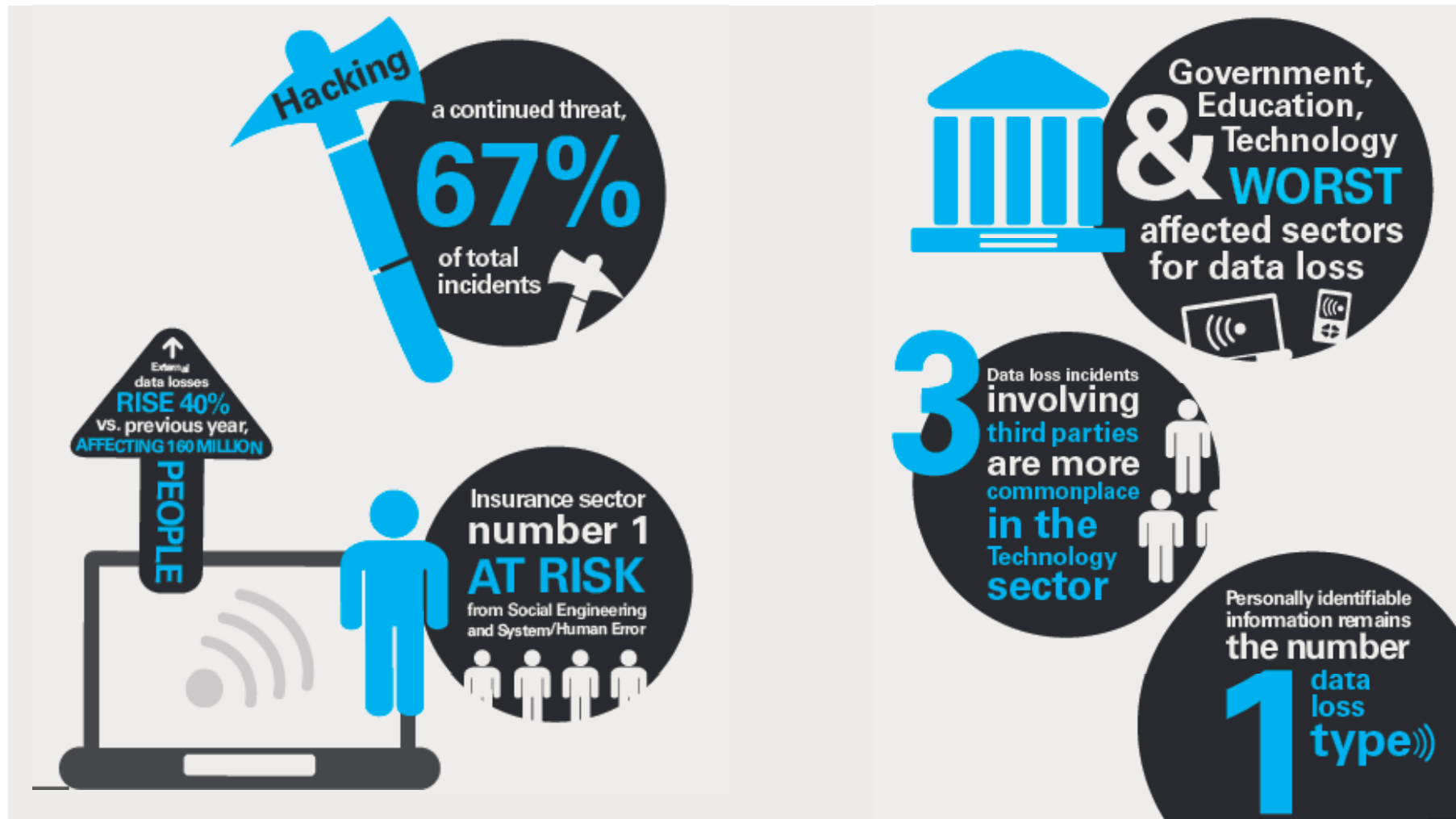
cutting through complexity

Technology challenges and considerations with Privacy Amendment Bill

Presentation to Websense Privacy briefing

Wednesday 11 December 2013

Data loss – how bad is it?



Source: KPMG Data Loss Barometer 2012, <http://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/data-loss-barometer-2012.pdf>

Which key changes in the Privacy Amendment bill are likely to impact technology?

From

Adequacy approach

Cross-border disclosure prohibited
'unless'...

No mandatory data breach
notification requirement

To

Accountability approach

Cross-border disclosure permitted by
default with disclosure and consent

???

Compliance with the APPs requires organisations to know:

- **What** Personally Identifiable Information (PII) is held?
- **Where** it is located?
- **Who** has access?
- **How** it is secured?

Certain factors increase the difficulty in complying with these requirements

Key drivers



High degree of outsourcing and use of external suppliers

PII is both provided to and accessed by suppliers

Location / jurisdiction of data and personnel increasingly fluid

Additional factors



Low levels of staff awareness regarding the privacy requirements of PII and understanding what PII is

'Customer experience' can override privacy and governance controls

Data management practices struggle to keep abreast of the evolving environment

A **complete view of all suppliers** and their relationships can be **difficult to obtain**

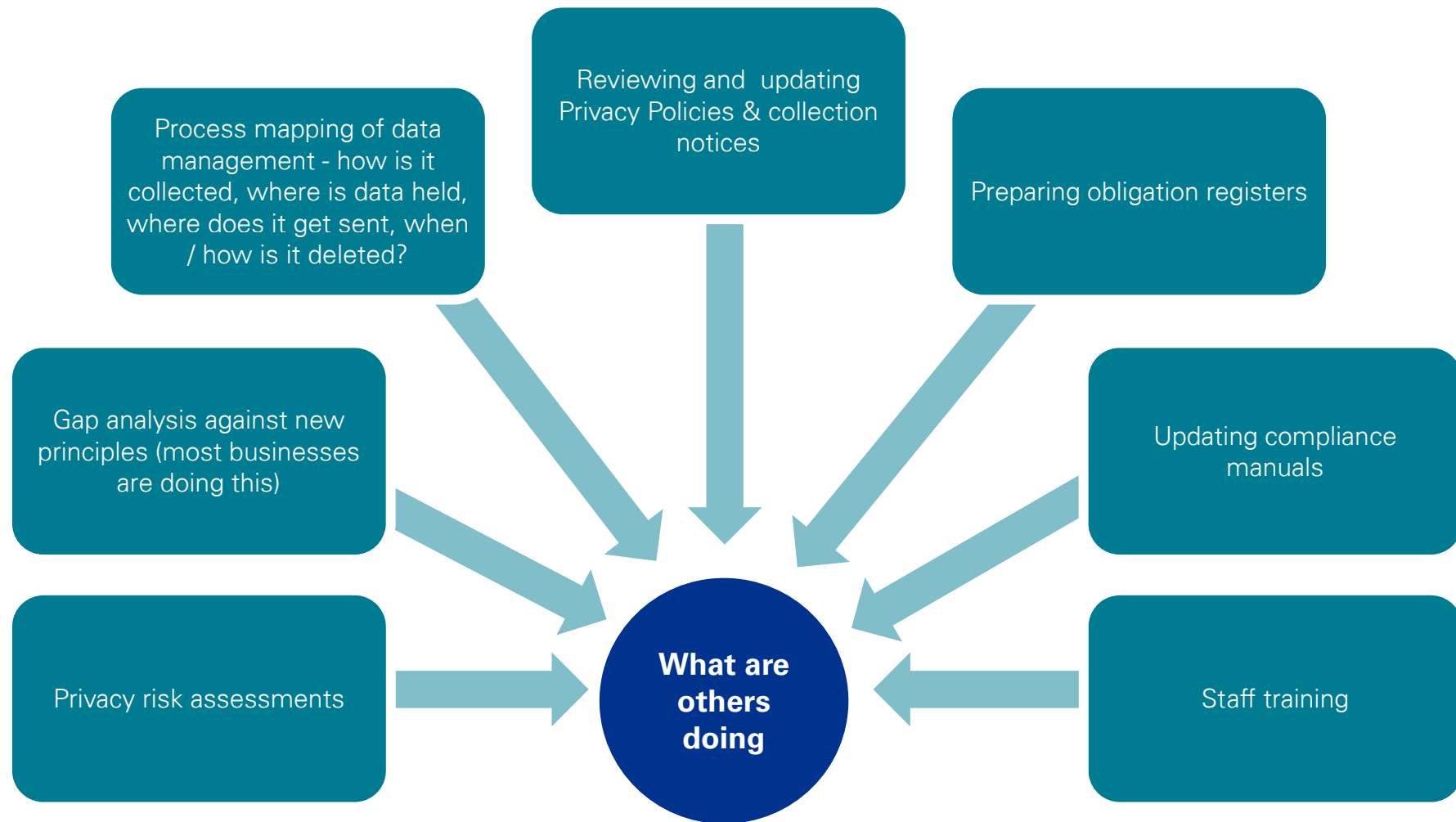
From our experience, there are many areas where PII may be unknowingly transmitted or stored outside of core systems.....

	Customer / Client / Patient PII		Employee PII	
Internal	Data warehouses	Development and testing environments	Performance management / payroll spreadsheets	Crisis management repositories
	Local folders, drives and email	Tapes and DR technologies	Active Directory & Email	Reward and recognition systems
External	Data enrichment providers	Mailing houses / Document scanning providers	Corporate travel company	Business card printer
	Service providers (incl. previous + PoC)	USB keys and portable hard drives	Corporate card provider	Hotels and airlines

What should IT be doing?

Action	APP
Determine whether a PII data inventory exists	All APPs
Determine why data is in these locations and how it is secured	All APPs, particularly and APP 11 – Security of personal information
Understand which service providers hold or have access to PII, and identify the jurisdiction of both the service provider and where the data is held / accessed	APP 8 – Cross border disclosure of personal information
Review contracts and Service Level Agreements (SLAs) to make sure responsibilities and controls for the protection of data are clear, robust and auditable	APP 8 and APP 11
Confirm policies and procedures for the following: <ul style="list-style-type: none"> • Data lifecycle • Systems lifecycle • Vendor lifecycle 	APP 11 APP 11 APP 8 and 11
Ensure your staff understand the privacy requirements on them – or at a minimum they know who to ask for help	All APPs, particularly APP 1 – Open and transparent management of personal information and APP 6 – use or disclosure of personal information
Regularly test your security – focusing on the risk areas identified in the inventory above	APP 11

What should be occurring across the organisation?



Two key messages to improve the likelihood of compliance to the new requirements...

- **What PII is held?**
- **Where it is located?**
- **Who has access?**
- **How it is secured?**

Provide staff and service providers with the tools to manage PII securely



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2013 KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.

Liability limited by a scheme approved under Professional Standards Legislation.