Cyber Security: Accidents will happen - Is your business prepared?

30 October 2015

Peter Bullock, Partner
peter.bullock@pinsentmasons.com

Pinsent Masons

Agenda

- Awareness
- Preparedness
- Pre and Post incident best practice
- Reputation management
- Clean up

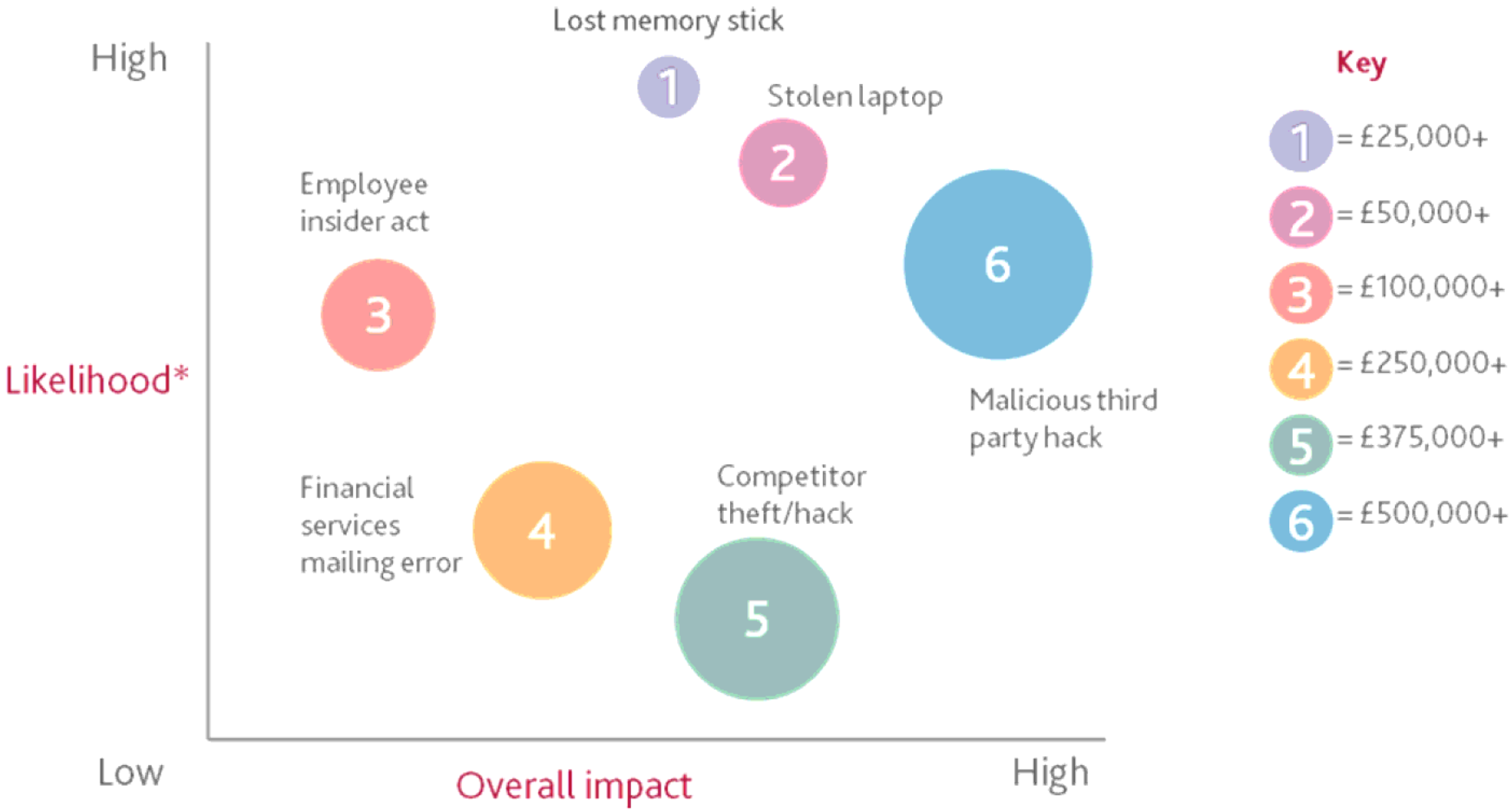
Awareness

- intentional
  - script kiddies
  - zero day bugs
  - activists (anonymous)
  - Industrial espionage
- unintentional
  - human frailty
- collateral
  - supply chain disturbance

Connected risks

- Sybil Logic Bomb Cyber Catastrophe
  - Cambridge Centre for Risk Studies stress test scenario
  - worst case: 5 year loss of US$15 trillion (bigger than 2008 financial crisis)
- this is not Y2K

Relative cost of incidents



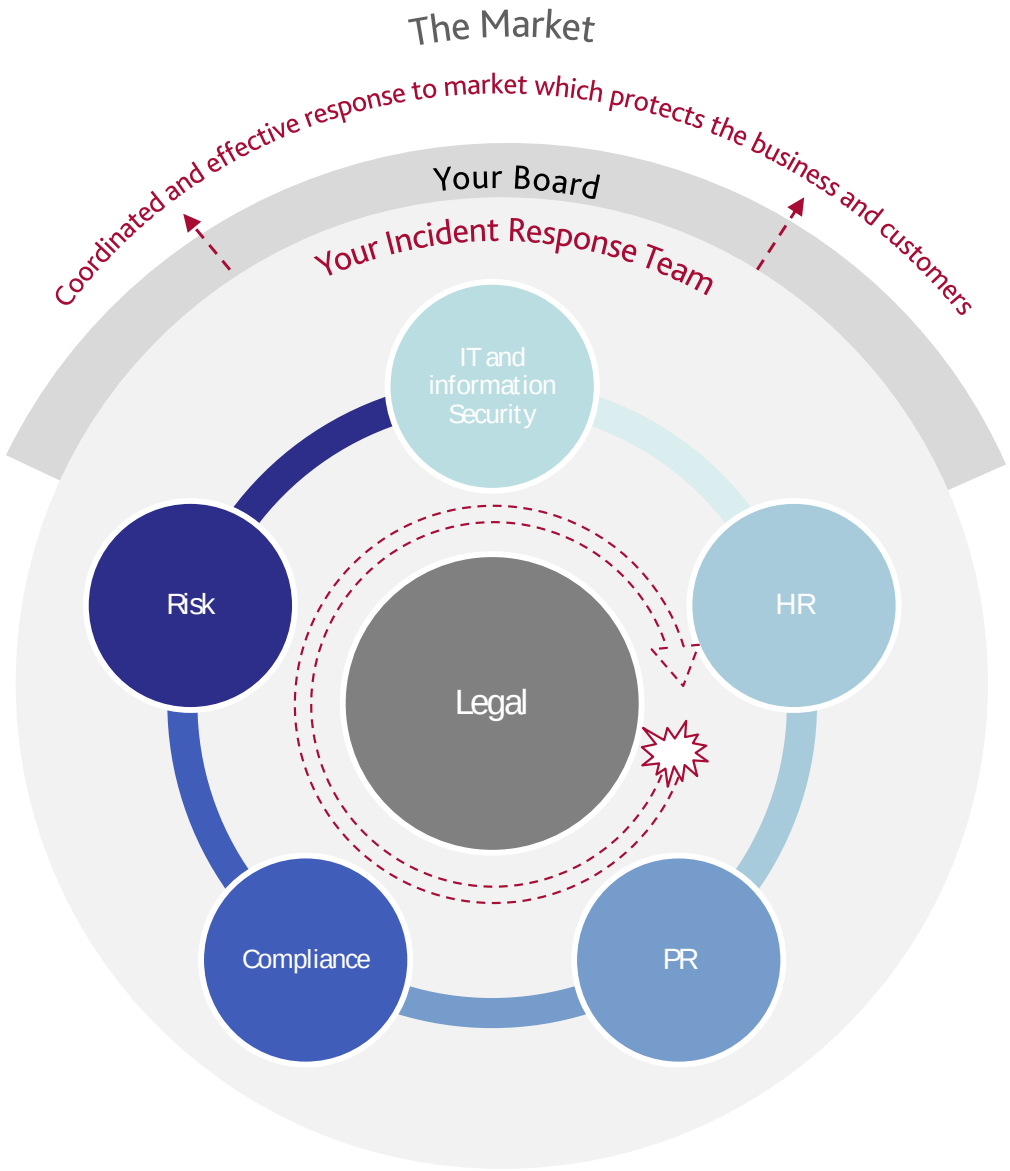
Pinsent Masons

Regulators wake up

- Hong Kong Monetary Authority
  - 15 September 2015 wrote to all CEOs of all Authorised Institutions
  - "*A credible benchmark of cyber security controls*"
  - pointing to international standards and other guidance
  - "*certain conventional risk management philosophy and controls practised by AIs might need to be adjusted or enhanced to cope with the risks*"

HKMA – 4 areas for cyber security risk management

- risk ownership and management accountability
  - not just IT
- periodic evaluations and monitoring of cyber security controls
  - it's a moving target
- industry collaboration and contingency planning
  - intelligence sharing
- regular independent assessment and tests
  - not just in-house expertise; penetration tests?



Pinsent Masons

Preparedness through simulation exercise

Stage 1: Preparation and fact finding

Stage 2: Designing and tailoring realistic hypothetical simulation exercise

Stage 3: Simulation exercise for Incident Response Team
Limited details at outset; further information by way of "injects"

Stage 4: Reporting: gap analysis

Pre-Incident: Best Practice

- Review key policies, e.g. IT security, information security, employee contracts / handbook
- Devise information asset register - attribute values
- Cyber insurance policies
- Review key contracts, e.g. suppliers, outsource providers and third party hosters
- Design Incident Response Plan
- Form Incident Response Team
- Conduct Incident Response Rehearsal(s)
- Set up a network of experts / vendors including legal, forensic, PR and credit monitoring services
- Due diligence and testing including penetration testing

Post-Incident: Best Practice

- Assemble Incident Response Team
- Evaluate the risks (legal, financial, reputational and technological)
- Follow Incident Response Plan including reputation management strategy
- Engage experts (legal, forensic, PR)
- Maintain communication amongst relevant stakeholders (management, PR, IT, compliance, legal) subject to legal privilege wherever possible
- Learn lessons and take proactive steps to reduce the risk and impact of any future incidents

Multiple data locations

Copied rather than ‘moved’

Replicated for availability, integrity

Same / different data centres (often 2 / 3 copies)

Data in persistent storage vs in processing (by applications)

Processing operations - replicated to different locations, for availability

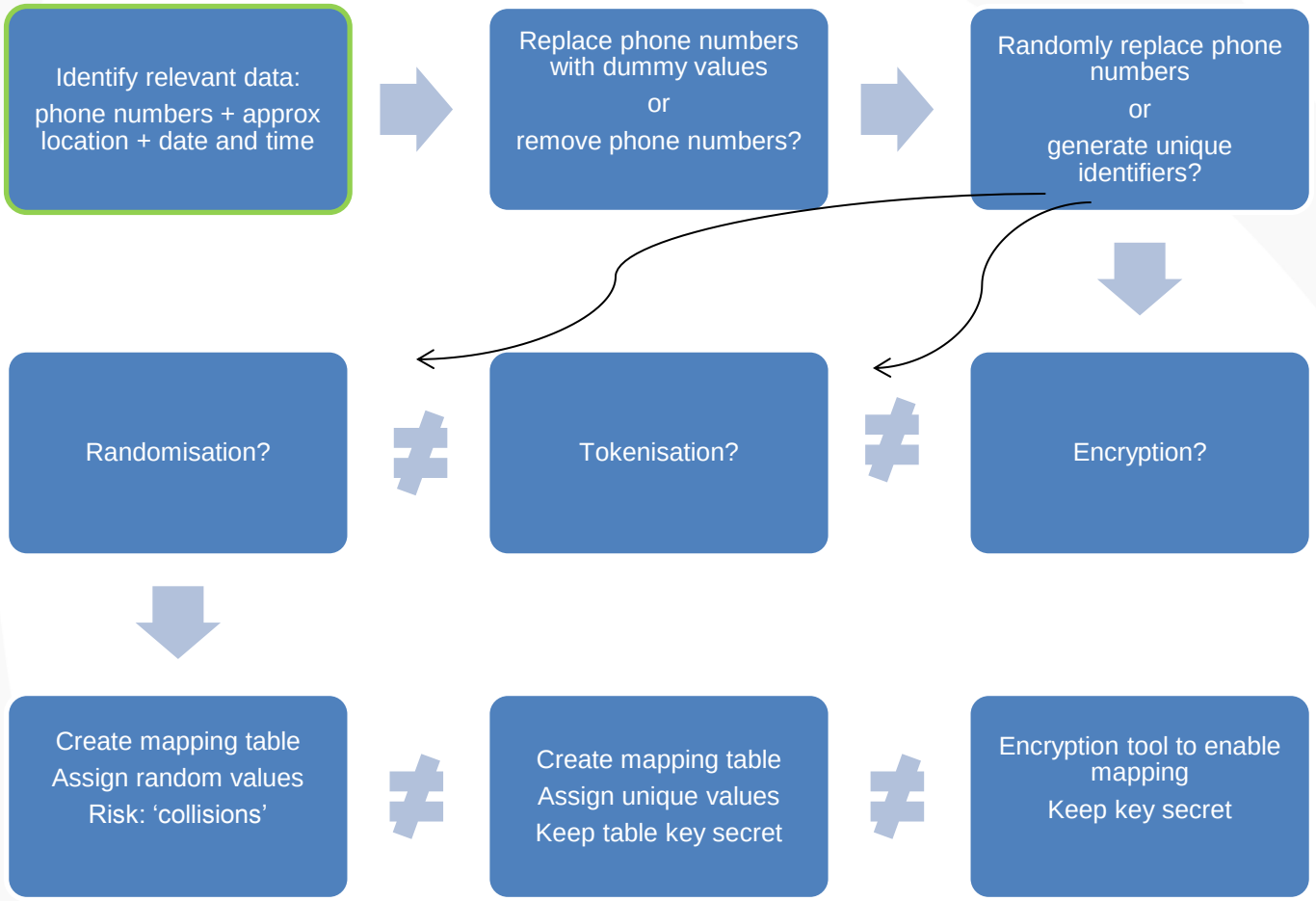
Caches, CDN edge locations etc

‘Pipes’…

Location realities

Locations multiple, may change	Control of logical access to intelligible personal data	Physical location not necessary / sufficient to control
EEA location does not guarantee protection	Hacking, foreign access e.g. US search warrants	Encryption + back-up considerations
Barges in international waters	Drones above regulated airspace	Supplier willingness to share server locations

Is it truly anonymised data?



Pinsent Masons

Managing the incident

** Notification may be required earlier to meet regulatory obligations.*

Pinsent Masons

Reputation

"*87% of executives rate reputation risk as more important than other strategic risks. 88% of executives say their companies are explicitly focusing on managing reputation risk*"

Deloitte – 2014 global survey on reputational risk

Notification

- cyber attacks often trigger intense scrutiny from regulators
- tough decisions need to be made about notifying those potentially affected
  - strict legal position on breach notification is fragmentary
  - it is about to solidify in Europe
  - regulators' positions are hardening
  - social media takes it out of your hands
- evidence needs to be preserved

An example

- over half a million CVs stolen from recruitment agency's database, hosted by its outsource service provider
- organised crime syndicate, working with an insider at the service provider, perpetrated the attack intending to sell the stolen personal data on the dark net

Response

- assessment
- devised website FAQs for affected individuals
- developed contact centre scripts
- credit monitoring services to individuals affected
- forensic advisers retained to investigate technical environment
- liaison with privacy regulators
- liaison with PR team

Further Information & Contact Details

Any questions?

Peter Bullock

Partner, Head of Technology and Dispute Resolution,
Asia Pacific

T: +852 2294 3438
M: +852 9104 5966
F: +852 2845 2956
E: peter.bullock@pinsentmasons.com

Pinsent Masons