DATA PROTECTION COMMISSION

Building Integrity and Trust

FREEDOM AND JUSTICE

MINISTRY OF COMMUNICATIONS

2017 DATA PROTECTION CONFERENCE

DATA PROTECTION COMMISSION
Building Integrity and Trust

MINISTRY OF COMMUNICATIONS

Ensuring Privacy in the Cloud

Mr. Michael Mudd, Managing Partner, Asia Policy Partners LLC

A World of Change

Digital from Birth

Mobility

Sociial

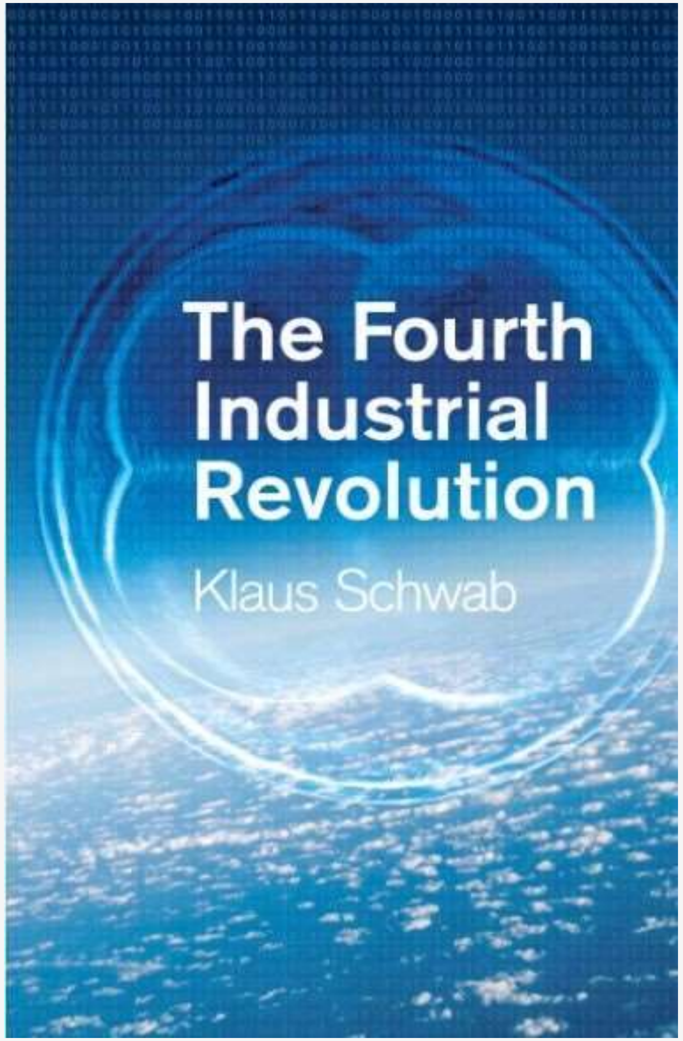
Data + Analytics

Data Driven Innovation

Environmentally aware

Service - Anytime, any place, any device, any channel - many delivered by some form of Cloud Service

https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab



The Fourth Industrial Revolution

Klaus Schwab

2017 DATA PROTECTION CONFERENCE

Online Security and Privacy Risk

- Global connections will hit 100 billion by 2025 – the ‘internetwork of everything’.
- Security risk planning for *all* losses -
  - Loss of Facilities, People, Data, Equipment, Intellectual Property Theft, denial of use.
  - Caused by: man made/criminal; natural; business; legislative.
- Privacy is a *data loss* risk.
  - Damage to business *relationships*.
  - Censure/fines from the *Privacy Regulator*.
  - Financial loss from a *reputational risk.*

Target Stores example (US)

- Date; Nov. 27 to Dec. 15 2013
- Massive loss of data; 40 Million customer records.
- Loss from the fraud ;$1.4-2.2bn*
  - … Does not include fines for loss of privacy.
  - … Or reputational damage.
  - … Card holders put on credit watch lists
- Data loss primarily due to inadequate data policy, aging on premise hardware/software and internal/external security controls.
- It cost the CIO then the CEO their jobs…

*Jeffries Securities 2014

Data as a New Currency ?

- No, I’m not talking about Bitcoin – yet.
- Data is what gives the new internet giants their valuation – Uber a booking service; $60+ bn?
- It is not just the collection of data, but how it is used to create value for both the data controller, those that contribute data and the end user.
    - Uber’s services cannot be used if the customer does not reveal their location.
    - Uber also uses public data – the GPS system.
- Data that is ‘hidden’, over classified or does not cross borders may not add value to an economy or a business.
- The challenge is how to protect the privacy and integrity of the data you hold and how best to manage it.

2017 DATA PROTECTION CONFERENCE

Data (Privacy) Loss Risk Management

- Build on “Assume Breach” as a foundational concept – you *will* get attacked sometime…
- Making sure the risk qualifiers used within your data loss mitigation strategy are similar to the ones used by your Enterprise Risk Management programme.
- Be crystal clear on who is responsible for data privacy controls of each department, who is responsible to deploy and monitor the controls.
- Ensure a very clear policy on escalation and managing disagreement (between your security manager and business line managers for example).

Data Classification and Privacy

- Not all data is created equal!
- Ensure that Data is classified according to importance and regulatory need.
- Example levels 1- 3*.
  - 1 – Low - Internal communications of low information content, customer facing, no encryption. No risk to the business.
  - 2 – Moderate - Internal/External communications, all PII moderate encryption. Medium Risk of data loss to reputation .
  - 3- High - Critical data such as admin. keys, back up keys high encryption. High Risk to the business with potential regulator intervention
- Email should be automated as to content above so the appropriate levels of encryption and controls are applied without user intervention or ability to override.
  - Mail server to automatically classify/encrypt emails containing PII etc).

erkeley.edu/da fication

Data/privacy loss threat classification

- Data theft – for profit (inc bank fraud/transfers).
  - Internal - IT/DC tech staff.
  - Internal - Other staff – admin/sales/management.
  - External – Suppliers/customers.
  - Other criminals.
- Data theft, alteration and/or destruction.
  - State sponsored.
  - Hacktivists.
  - Terrorism.
- Extortion.
  - Data encryption (Ransomware).
  - Phishing/Spoofing/Vishing (may be part of for profit).

Policy driven data security enhances privacy

- **Build** - On the BASIC concept.
- **Create** – Clear policies that govern who should get access to data and when.
- **Access data** – Only at just the right time that is needed to deliver the service.
- **Enable Ability** - To change access rules on the fly as business or job role changes.
- **Enable Access –** Create rules dependent on the environment - Fixed or mobile for example.
- **Enable Flexibility** - To prevent unauthorised file sharing, shadow IT, social media risk.

International Observations of Breaches and Strategy/1

- Most relate to finance/insurance companies.
- Theft of equipment, servers, notebooks CDR’s.
- Irish DPA established a Multinationals and Technology team to coordinate CB issues and to encourage “privacy by design’.
  ‘https://www.insideprivacy.com/international/europeanunion/irishdataprotectioncommissionerreleases2016annualreport/rivacy by design
- Looking at contracts in advance from companies outsourcing.
- EU GDPR guidance being looked at closely prior to May 2018.
- Very few, if any breaches related to a Cloud failure.

International Observations of Strategy/2

- Most DPA’s look for legal equivalency for cross border data flows.
- Similar to financial services, common messaging rules – SWIFT.
- In physical trade the HS Codes take friction out of paperwork.
- Similarly for digital trade, when data flows to scale on demand, it will increase efficiency through transparent rules on CB data flows.
- Clear guidance for the Data Controller and the Data Processor will ensure better compliance and control.
- Ghana may take a lead here based on work done to date.

Global Standards - ISO

- ISO 38500 Governance of IT for the organisation.
- ISO 27000 series for IT operations is most relevant for cybersecurity protection.
- ISO 27017: is the latest standard for Cloud information security controls.
- ISO 27018 is an international standard, for Privacy in the Cloud to protect personal data.
- ISO/IEC 18033 – specifies encryption of data.
- The ISO 31000 series – Enterprise Risk Management including governance bring together security risk management and resilience.
- Others- COBIT, PRINCE 2; sector specific; e.g. HIPAA.

2017 DATA PROTECTION CONFERENCE

Privacy and the Cloud

- Remember that 100 billion connections?
- Most are *already* in the Cloud.
- The Cloud is transnational in nature;
  - Multijurisdictional privacy laws apply.
  - Subject to both laws of origin of the data and where the data resides.
  - Data Controllers may specify where their date resides overseas
- Cloud Service Providers (CSP’s)
  - 4 global.
  - 3- 4 midsize.
  - many national.
- ISO and sector privacy standards with end to end encryption, enable safe cross border exchange of data to the same standards as financial services.
- Contract key to service delivery, data integrity, security and privacy.

How the Cloud enhances privacy

- Data security improved as the Cloud enforces data governance through centralized rules.
- Constant updates 24 x 7 identifies and traps malware that steals personal information before it infects data.
- Email/messaging scanned before delivery reducing risk of phishing.
- OECD/ENISA states; "…ability to dynamically upscale security resources…".*
- Resilience advantages in dealing with attacks due to geographic replication abilities.

* https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computingbenefits-risks-and-recommendations-for-information-security

Conclusion

- Privacy protections are enhanced by a Data Management Strategy.
- Data Privacy Protection - Protect what is important - not just data.
- Global standards assist in data governance.
- Privacy and Data Classification help realize your data’s full value.
- Cloud computing enables safe cross border data exchange.
- Clear guidelines as to data protection equivalency improves privacy.
- An enhanced - and compliant - data privacy strategy can be built using the Cloud.

About the Speaker

Michael Mudd

Managing Partner, Asia Policy Partners LLC

Michael (Mike) Mudd is the Managing Partner of Asia Policy Partners LLC (APP) an ICT data strategy , privacy and cybersecurity policy advisory firm providing thought leadership on business transformation through technology which he founded in 2010. Prior to this he held leading commercial positions with Riverbed Technology and Standard Chartered Bank PLC, joining the bank from Noble Group, a global commodity trader.

An appointed technical expert to the ISO and a member of the Government of Hong Kong's Expert Group on Cloud Computing, Security and Privacy Advisory Committee. He holds positions on IT Policy, FinTech and Cloud in the Hong Kong Computer Society as well as OSAC, Hong Kong and is the co chair of the IT, IP and Telecom Committee of AmCham in Hanoi, Vietnam.

He is the chief representative of the UK based Open Computing Alliance for Asia Pacific , the Middle East and Africa. He also participates in the work of APEC in several working groups on digital trade and technology. asiaitpolicy@live.com

Thank You!

Michael Mudd

Managing Partner, Asia Policy Partners LLC

technology : policy : compliance: training

asiaitpolicy@outlook.com