SESSION 2: RISK MANAGEMENT IN THE DIGITAL ERA

WIN In-House Counsel Day Canberra 2017
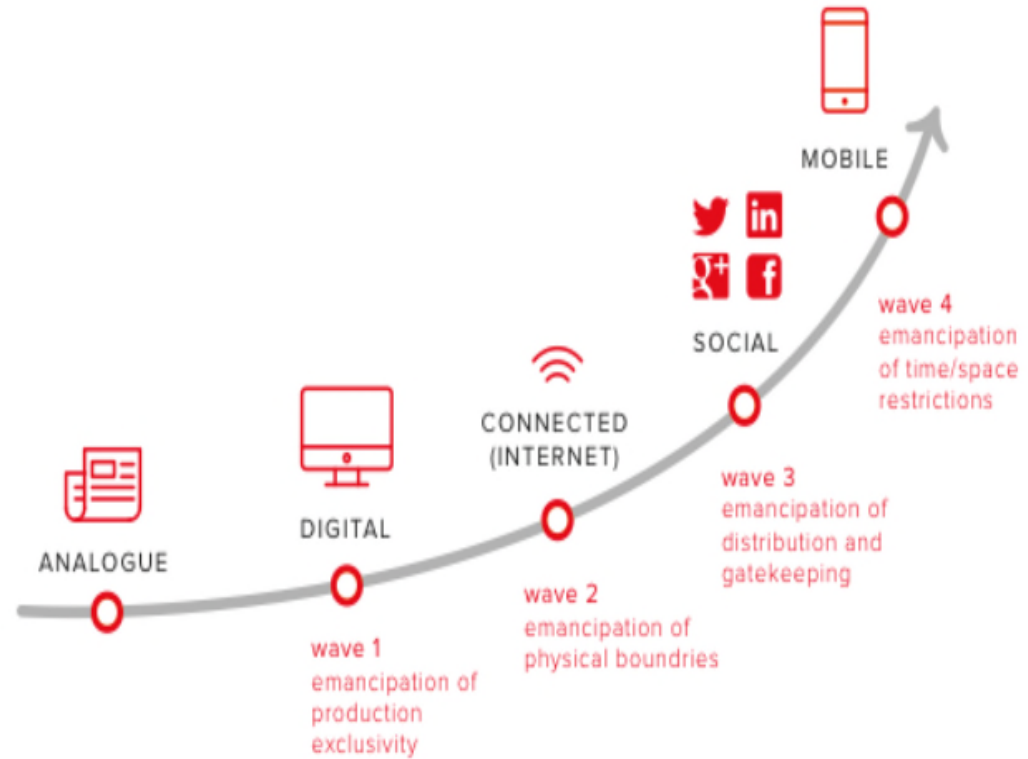
Friday, 24 February 2017

DLA PIPER

What risks does your business face in the digital age?

A fast changing landscape

- Big data
- AI
- IoT
- Cloud computing
- Social media
- Increase in data breaches and ransomware attacks

MOBILE

SOCIAL

CONNECTED (INTERNET)

DIGITAL

ANALOGUE

wave 1
emancipation of
production
exclusivity

wave 2
emancipation of
physical boundries

wave 3
emancipation of
distribution and
gatekeeping

wave 4
emancipation
of time/space
restrictions

What are we going to cover?

- Conduct Risk – Ethics & Reputation
- Information Risk - Confidentiality & Data Protection
- Social Media
- Cyber Security
- File Management
- Risks from other parties
- Opportunity for Innovation
- Health & Safety

Ethics and Reputation

"The principles are the same. The online world has just opened up new ways of breaching them."

Law Society of NSW, March 2015

Reputational Risk

Every document, email, tweet or social media posting has the potential to be circulated worldwide in the digital age, and its footprint will remain forever.

Reputation – a precious commodity

Your regulatory and ethical duties

DO	DO NOT
Maintain high standards in everything we do	Seek to avoid responsibility for our actions
Deal in open, fair and objective way	Undertake work for clients through a misguided sense of loyalty
Give clients (whether internal or external) clear guidance on requirements	Continue working for a client without addressing any ethical concerns (and escalating appropriately)
Follow all policies and procedures	

How might I unintentionally breach confidentiality?

- Lost personal laptop on plane which contains emails, sent to personal email account, which contain confidential, price sensitive information

- Lost unencrypted USBs

- Emails inadvertently sent to an unintended recipient

- Including derogatory comments about someone in an email/in writing

Practical tips

DO	DO NOT
Lock your computer when not in use and keep your desk clear of sensitive materials	Discuss work matters on social media
Proof read your emails before hitting "send"	Send sensitive confidential information to personal email accounts
Use confidential waste bins and/or shredders	Leave confidential materials on the printer or photocopier
Encrypt and password protect USB keys, laptops, DVDs and CDs for external use	Share passwords
Ensure that your smartphone/tablet is safe and get in touch with IT if you lose it	

Your duties of confidentiality continue even if you leave the business

Privacy and data protection

- Know where your data is stored

- Know where your data is transferred/shared

- New General Data Protection Regulation (EU) in 2018 regulates all data transferred into EU

- Update privacy policies and employment contracts

Social Media

Social media in business

- Need to have a social media policy

- Provide guidance and training and how to use social media

- If you have social media accounts – make sure more than one person knows the account details
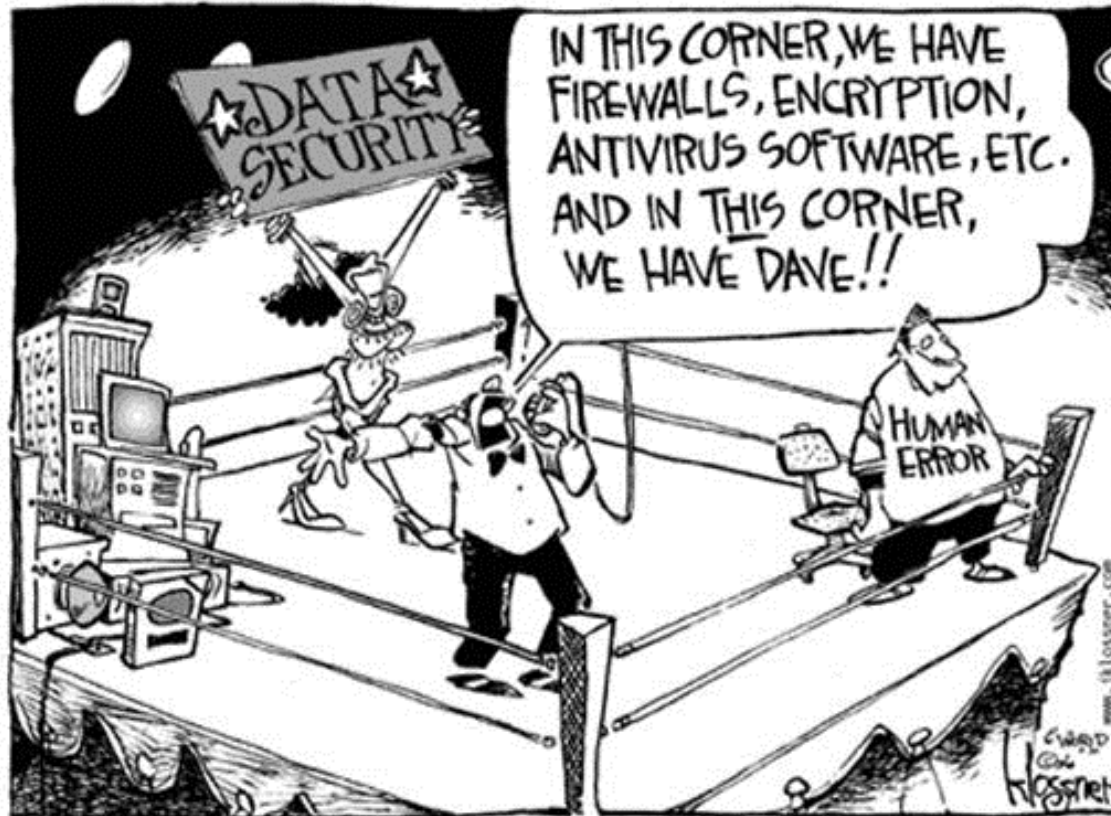
- Must monitor your accounts

Using information gleaned from social media

- When can you use information?
- Dangers

Cyber Security

What are the threats?

Threats
- Data theft for extortion, exploitation
- System / data sabotage
- Fraud - via web, email, phone, mail
- Identity theft for financial exploitation
- Client / regulatory compliance failure

Targets
- Email
- Financial Systems and data
- Documents: DMS, hard drives, USB
- Paper, physical premises

Actors
- Internal Personnel
- Criminals
- Nation States
- Terrorists
- Hacktivists

Data Breach or Loss

- Use of Drop Box and other file sharing sites

- Use of Wechat and other informal communication channels

- Scam emails

- Phone calls

- Passwords

How to respond?

- Get close to your IT department and make sure they are skilled up

- Consider external audit/assessment of cyber defences

- Identify high risk clients and matters at inception

- Agree with client any additional security that might be required (eg encryption, passwords etc)

- Training and awareness (e.g. e-learning and targeted phishing campaigns)

- Know who the cyber experts in your firm/company are and harness their expertise and commitment

- Adopt cyber incident response plan and get high level buy-in

- Have list of cyber responders ready

- Consider cyber insurance

Challenges of File Management

- People are working on the go, online all the time
- BYOD
- People using non-company apps, such as note taking apps, over which company has no control
- Use of social media or messaging applications Whatsapp, WeChat etc
- Using personal email accounts or storage sites such as Dropbox, Box, GoogleDrive, OneDrive

Solutions for file management

- Education and awareness

- Policy and guidance – electronic vs paper filing or hybrid

- Mobile management solution for BYOD to secure information

- Easy file solution which allows emails to be filed on the go and/or 'send and file' option

- Apply appropriate security controls for highly sensitive information – information barriers

- Consider inbox clean up processes for leaving employees

- Data retention period for hard copy and electronic files

Risks from other parties

- Potential to jeopardise your data protection standards, access to information or systems

- Potential impact on your reputation

Opportunity for Innovation

- Digital changes bring vast opportunity to those at the forefront
  - AI
  - Big data
  - Harnessing social media
  - Outsourcing
- Culture of innovation

Health & Safety

- The 'Ergonomic Tsunami'

- Resilience in a high performance culture

WHAT RISKS DO I FACE?

Act now:

- Raise awareness – education, communication and sharing information about near misses

- Training - e-learning and classroom based training

- Get close to your IT department – know what is going on

- Identify very sensitive information and secure appropriately

- Encrypt your devices

- Stay informed and well connected with others

- Don't get let behind!

Helpful resources

- Law Council of Australia – new cyber site -
  http://lawcouncil.asn.au/lawcouncil/cyber-precedent-home

  - Bite sized videos

  - Checklists for how to respond to cyber attack or considerations about using the cloud

- Australian Cyber Security Centre – government site https://www.acsc.gov.au/

- Insurers/brokers – useful information

Questions?