GDPR, NIS Directive, etc etc: will they drive organisations to improve their security posture ?

fieldfisher

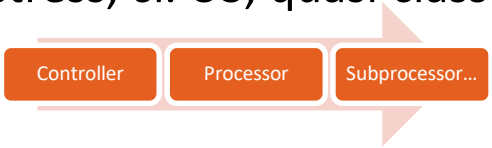
Dr W Kuan Hon

Director - Privacy, Security & Information Law

19 June 2019, EEMA's 32nd Annual Conference

Security – GDPR **sticks** and **carrots** – biggest area (with DS rights)

- Regulatory fines – 2 tiers – aggravating / mitigating factors
- Compensation: incl. distress, cf. US; quasi-class actions
  - Supply chain risk



- Operational disruption
- Reputational damage, jobs etc.
- GDPR-approved certifications
- GDPR-approved codes of conduct
- Selling point / competitive advantage ?

- Controllers
- Processors

- Certification body
- Monitoring body

GDPR & security-related requirements (see Encyclopedia of Data Protection & Privacy)

- Security / data protection measures “appropriate” to risks to data subjects particularly I&C, including “as appropriate”: pseudonymisation & encryption, CIA, resilience, timely recovery, regular testing - and see NCSC / ICO GDPR security outcomes
- Integrity & confidentiality – higher-tier, controllers
- “Personal data breach” notification: also WP250
- Employees / subcontractors
- Supply chain – due diligence etc.
- DPbDD, DPIAs – incl. **procurement** of **secure hardware** and **software**
- Accountability - http://bit.ly/accountabilitysong !
- (NOT “transfers” ! – see Data Localization book)

GDPR - UK

- ICO first year report – 14k PDB to 1 May 2019 - nearly 4x; < 0.5% improvement plan / fine. Not yet for security
- UK FTSE 350 Cyber Governance Health Check
  - 77% increased **board discussion & management of cyber risk** since GDPR introduced, and 55% **increased measures**
  - Indeed 41% of businesses **increased measures** in response to GDPR, and those were more likely to **test crisis plans regularly**, and to have **involved the board** in a crisis simulation exercise within the last 12 months
- UK Cyber Breaches Survey 2019
  - **30%** businesses and **36%** charities **changed cyber security policies / processes** as a result of GDPR - GDPR has encouraged and compelled some organisations over the past 12 months to **engage formally with cyber security for the first time**, and others to **strengthen their existing policies and processes**
  - **Fall in numbers identifying breaches / attacks**: "GDPR might have changed what businesses consider to be a breach, or led to some businesses becoming less willing to admit to having cyber security breaches…"
  - And - some organisations frame cyber security largely in terms of **avoiding PDBs**, less focused on other kinds of breaches or attacks, narrower set of technical controls - e.g. cyber vs. supplier
    - Due diligence - some supplier checks focused on GDPR compliance & PD, cf. cyber security more generally
  - **On balance, positive impact** on cyber security, but organisations may need to think **more holistically**

NEW !

Security - lessons from GDPR fines to date

- https://www.linkedin.com/pulse/security-lessons-from-gdpr-fines-dr-w-kuan-hon

- https://privacylawblog.fieldfisher.com/2019/security-lessons-from-gdpr-fines

EU NIS Directive & Implementing Regulation; UK NIS Regulations

- Operators of essential services (OESs) & (lighter-touch) digital service providers (DSPs) - requirements regarding:
  - Security measures – not just cyber ! Accountability
  - Incident notification
  - NB. **contracts**
- **National** penalties - compensation, criminal liability etc ? – e.g. UK – GDPR-level fines
- Reputational risk – lose customers, jobs etc.
- Selling point / competitive advantage ?
- Any improvement ? Too early to tell…

Another example: FS regulation - Tesco Bank

- FCA fine - £16.4m – debit cards fraud
- Principle 2 - conduct business with due skill, care and diligence – incl. response (cf. security)

NCSC's Cyber Ps for the Boardroom

- Phishing
- Privileged accounts
- Patching
- Providers / partners / processors
- Passwords / authentication

- + Publicly available inadvertently…?

Fieldfisher's free GDPR app

- Android
  https://play.google.com/store/apps/details?id=com.fieldfisher.gdpr

- iOS
  https://itunes.apple.com/gb/app/gdpr-the-complete-guide/id1239256607?mt=8

Thank you ! Questions ?

Dr W Kuan Hon

Director, Privacy, Security & Information

Fieldfisher

T: +44 (0)207 861 4545

M: +44 (0)739 1419 940

E: kuan.hon@fieldfisher.com