janet

# Protecting Valuable Research Data

Andrew Cormack
Chief Regulatory Adviser, Janet
@Janet_LegReg

# Valuable data

janet

- Including
  - Commercially exploitable (by us, or others)
  - Politically sensitive (e.g. Financial or climate modelling)
  - Sensitive data from others (e.g. Health)
  - Legally/ethically sensitive data generated here (health, criminology,...)
    - For security-sensitive data, see UUK (2012) report
- Potential target for
  - Competitors
  - Activists
  - Criminals
  - States
  - ...

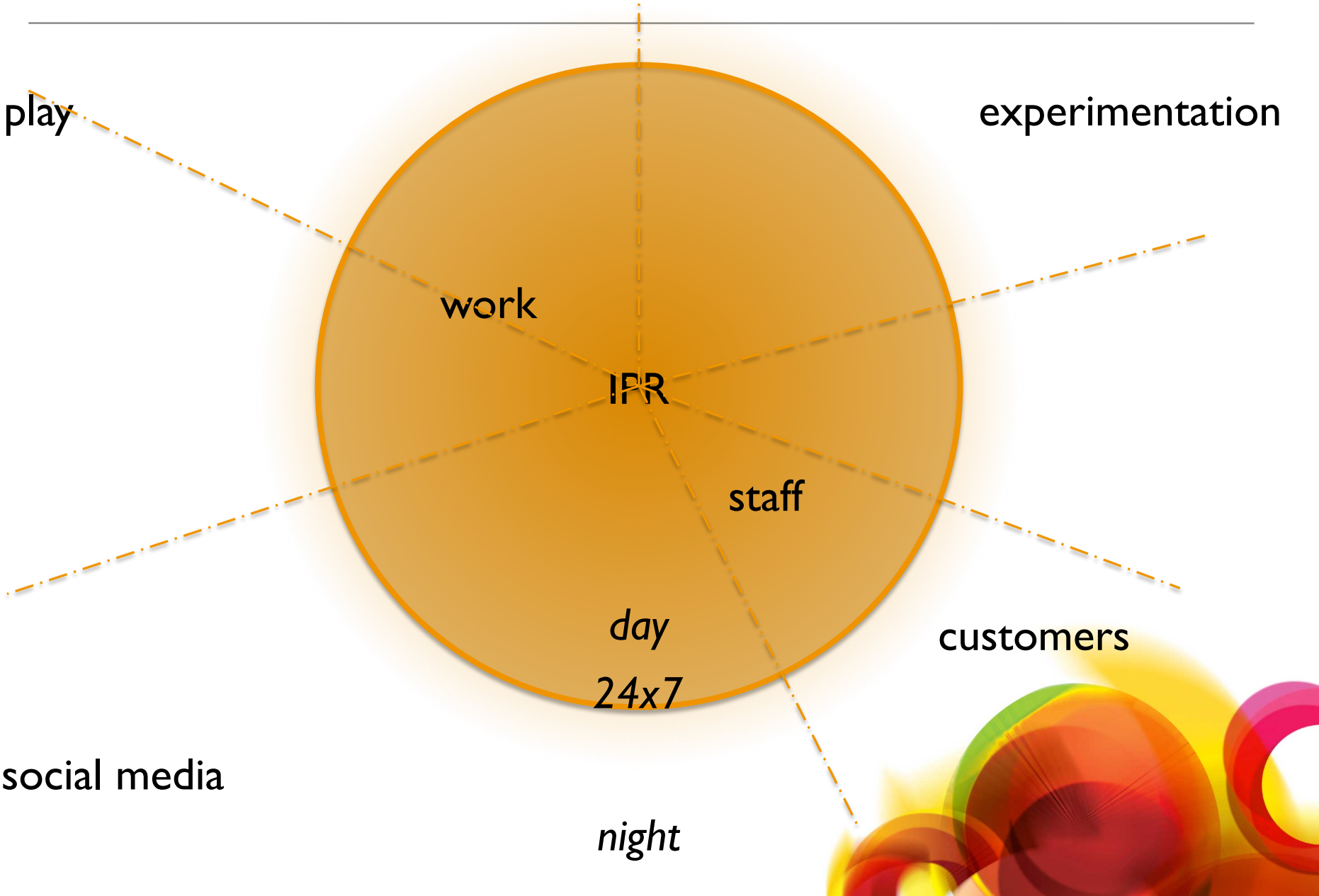
# Only valuable if it can be used

janet

- Which requires
  - Transfer across our networks
  - Processing by our people
  - Using our systems
- Same networks/people/systems also need to support
  - Innovating
  - Learning
  - Administering
  - Living

# The "university" model

janet



# The university model

janet

# Thinking about solutions...

janet

- BIS, Cabinet Office, CPNI, CESG
- Cybersecurity Centres of Excellence
- Heads of Research Administration
- Heads of University Administration
- UUK, RUGIT, UCISA
- Janet

# Technology conclusions (facilitated by RUGIT)

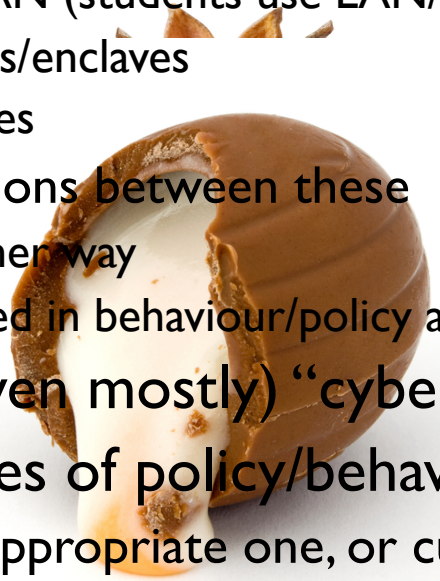
janet

- Almost all CPNI/SANS Top 20 measures already used in HEIs
- Some appropriate across whole organisation
  - Vulnerability assessment, wireless device control, backups, router security, port/protocol controls, boundary defence, logging, secure network engineering, incident response
- Some appropriate for secure enclaves
  - Device inventory, software inventory, secure hw/sw configurations, malware defences, application security, admin privileges, critical data, account auditing, data loss prevention, pen.tests,
  - BUT in wrong place, these could encourage insecure behaviour ☹
- Only one missing
  - Universal security skills assessment, awareness and training ☹
- Top 20 is a guide, not a compliance standard

# Network conclusions (facilitated by Janet)

janet

- "Whole enterprise" approaches don't fit
  - Hard shell/soft centre ☹
- Welcome the pomegranate (credit a previous speaker!)
  - There is a (wrinkled) perimeter, containing
    - Not very trusted LAN (students use LAN/wifi/3G interchangeably)
    - Some sensitive seeds/enclaves
    - Some hazardous ones
  - Lots of internal partitions between these
    - Which may face either way
    - Must be implemented in behaviour/policy as well as technology
- Threat not just (or even mostly) "cyber"
- Need to offer packages of policy/behaviour/technology
  - Risk owners choose appropriate one, or customise



# Organisations (led by UUK)

janet

- Three step process
  - Assess institutional risk
  - Effective oversight/reporting: board+owners+controllers+users
  - Target appropriate/proportionate controls at vulnerable assets
    - Over-strict controls/over-broad scope encourage risky behaviour
    - Right policy/behaviour/technology in secure enclaves
- Should be normal data management policy/practice/culture
  - Led by research managers, principal investigators, governors
  - Implemented by all staff and students
    - Key roles both in assessing risk **and** in implementing controls
  - Satisfying funders: "this is how we protect it, OK?"
- Publication/open data means
  - Focus on integrity, confidentiality and availability
  - Security requirements as part of data lifecycle

# Conclusions

janet

- It's about people and organisations
  - Supported by policy/behavioural/technical systems
  - Over-protecting increases risk
- It's already being done
  - Promoting academic freedom to get on with knowledge creation
  - Need to capture, support, disseminate that good practice
- We have the tools, you tell us where they are needed
  - Case studies/examples, please?

janet

# Questions?

Janet, Lumen House
Library Avenue, Harwell Oxford
Didcot, Oxfordshire
t: +44 (0) 1235 822200
f: +44 (0) 1235 822399
e: Andrew.Cormack@ja.net
b: https://community.ja.net/blogs/regulatory-developments

# References (and see UUK paper)


https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf

www.cpni.gov.uk/advice/cyber/Critical-controls/

www.rugit.ac.uk/meetings/presentationsnotes/november2013/CPNIControls-RUGITPaper.pdf

community.ja.net/library/janet-services-documentation/protecting-sensitive-information-workshop-report

www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf

www.dcc.ac.uk/resources/policy-and-legal/overview-funders-data-policies