Properly Safeguarding Data – How much security is enough?

Prof. Paul Dorey, Ph.D. CISM, F.Inst.ISP
Royal Holloway, University of London

1

My background & Purpose of the talk

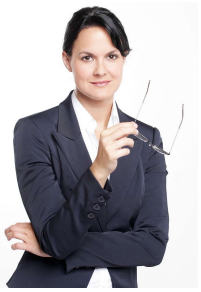
- Career as a CISO – Deutsche Bank, Barclays, BP, GSK and other related roles
- Visiting Professor in information security
- Advisor to CISOs, businesses & government
- Expert witness

- The challenge I see companies facing
- What security do regulators expect?
- A case study – nice surprises and the not so nice
- What you absolutely have to get right
- Challenges for the coming decade

2

Questions, Questions….

- Should we encrypt the data?
- What security do we have?
- What security do we need to have?
- What security is even possible?



- What are you talking about?
- What key length do we need?

Image credits: Angelo Esslinger, imperioame

3

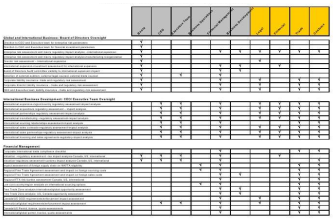
Challenges

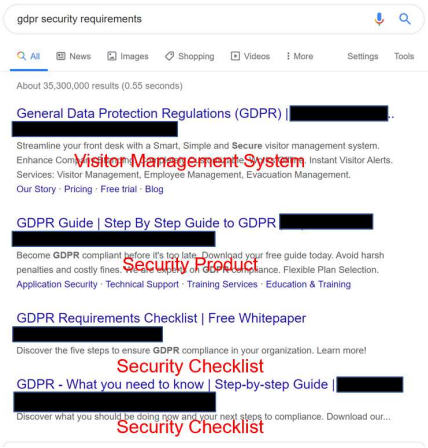
- Different knowledge between IT team and Privacy team
- Security is a multi-layered and multi-disciplinary problem
  - Technology
  - Processes
  - People
- Simple ‘tick box’ answers can be very misleading
- It is accepted that security breaches are inevitable
  - How can the impact of a breach be mitigated?
  - How can the company present a defensible position when it happens?
- So what does the GDPR say about security?
- What do the individual regulators say?

4

Common security approach

- Checklists
- Multiple Security Standards – e.g. ISO 27001, CSA etc
- Tools





Ensure IT environment meets GDPR

5

GDPR

Article 5(1)(f) [personal data shall be:]

'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

Article 32, 'security of processing':

'Taking into account the **state of the art, the costs of implementation, and the nature, scope, context and purposes of processing** as well as the risk of varying **likelihood and severity** for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of **security appropriate to the risk**, including inter alia as appropriate:

… (b) pseudonymisation and encryption of personal data'

6

GDPR

Recital 83 says:

'In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should **evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption**. Those measures should ensure an appropriate level of security, including confidentiality, **taking into account the state of the art and the costs of implementation** in relation to the risks and the nature of the personal data to be protected.'

So this is about **risk**….

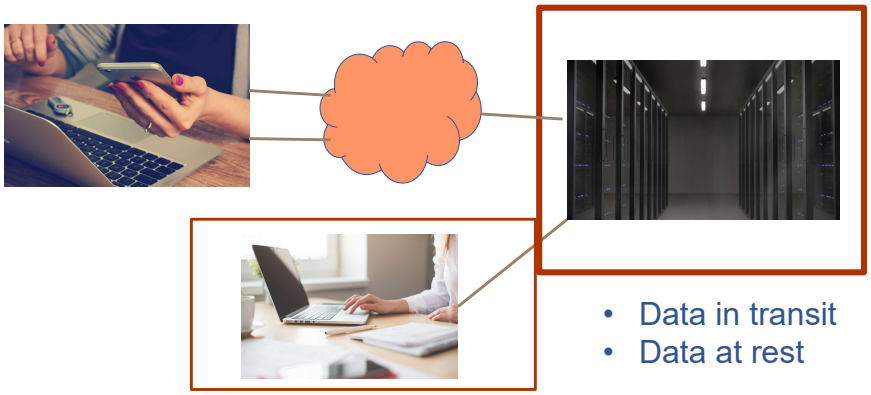
7

UK ICO

"The **GDPR does not define the security measures** that you should have in place. It requires you to have a level of **security that is 'appropriate' to the risks** presented by your processing. ... This reflects both the **GDPR's** risk-based approach, and that there is no 'one size fits all' solution to information security."

8

Risk:To encrypt or not encrypt?



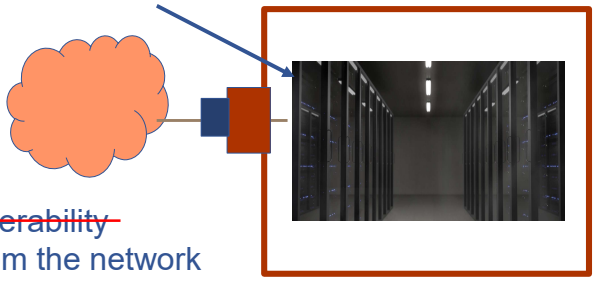
- Data in transit
- Data at rest

Photo credit: William Iven, Elias Sch , hamonazaryan1- Pixabay

9

Security trade-offs and risk

- A vulnerability has been reported…

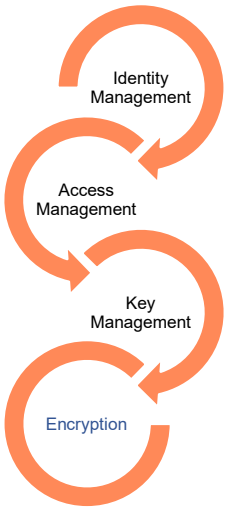


- ~~Patch the vulnerability~~
- Disconnect from the network
- Remove the vulnerable service
- Deploy a Web Application Firewall
- White-list the software on the device

10

Security implications and risk

Security Chain

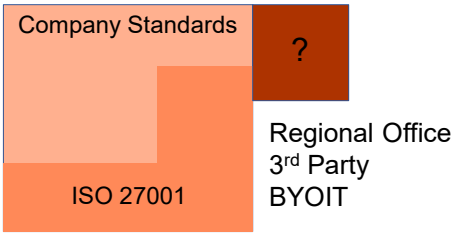


What we thought we could do..

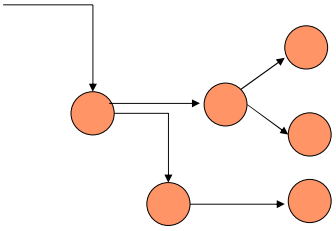
- We have created an inventory of systems holding PII
- We have a process assessing new systems and projects

- But have we looked at the information flows..
  ….. and the security surrounding those flows?
- Is there an IT systems strategy which optimises the PII security solutions? (e.g. a secure storage service)
- How do we bring risk thinking into play?

Compliance Standards vs Flows



Regional Office
3rd Party
BYOIT



Who handles the data?
On what systems?
Via what communications?

13

Why not just address control gaps?

- Using lists of controls is fine – and gaps can have mitigating approaches recorded
- However:
  - Which of the many lists should you use?
  - High level questions get high level answers:

    Q:"Do you encrypt?" A: Yes

    (But what, and where and how/when decrypted?)

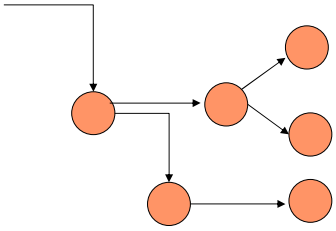
  - If you don't look at the information flow you may miss a set of security control requirements (different device, different organisation).

14

Case Study

Nice surprises

- End to end encryption

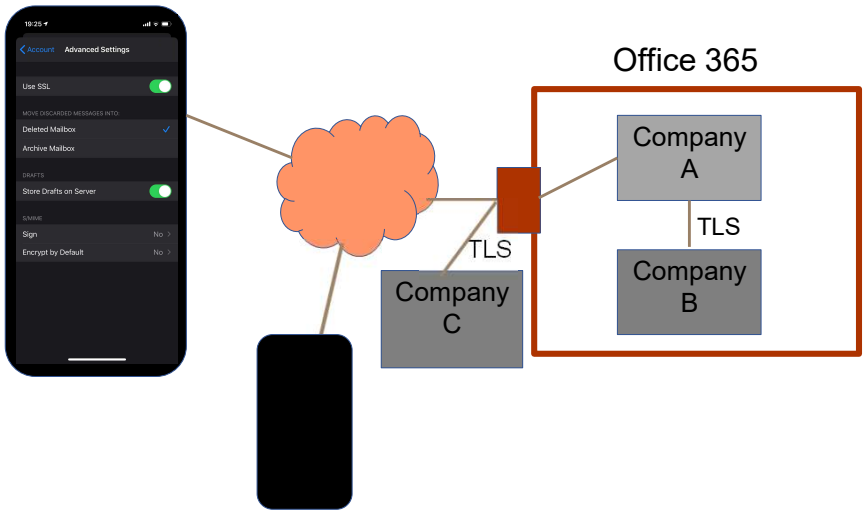


Still to do

- Complete 3rd party assurance
- Deploy alternatives to USB sticks
- Tidy up all cloud file stores

15

Nice surprise

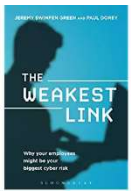


16

BUT – Secure environment is needed

What I look for….

- Security culture



Swinfen Green, Dorey,
The weakest Link,
Bloomsbury (2016)

- Good architectures, designs, standards, software
- System hygiene
- Detection and response
- 3rd party assurance
- Good governance (Risks identified and addressed).

17

What do I look for?

- Security culture – awareness, skills, behaviours
- Good architectures, designs, standards, software
- System hygiene – patched, configured, timely maintenance
- Detection and response – able to detect and mitigate
- 3rd party assurance – knowledge of state and performance
- **Good governance** – risk registers, decisions, tracked actions

- With ….Documentation!

18

Challenges for the decade

- Privileged user management
- Credential Management – Passwords to MFA
- Client device management - Intune
- Getting skills, establishing corporate oversight
  - Cloud
  - IoT
  - AI
- Achieving cyber resilience

19

In summary

- **Know the appropriate state of the art for security**
- **Know what the regulatory advice says**

BUT MOST IMPORTANT

- **Know the nature, scope, context and purposes of processing**
- **Look at the flows and assess the risk**
- **Establish security appropriate to the risk**

20

IT-Security-Privacy: Multidisciplinary

Success requires cross function collaboration within an integrated risk framework.

Image credits: Gerd Altmann

21

Thank you for your attention…

Questions ?

paul.dorey@rhul.ac.uk

22