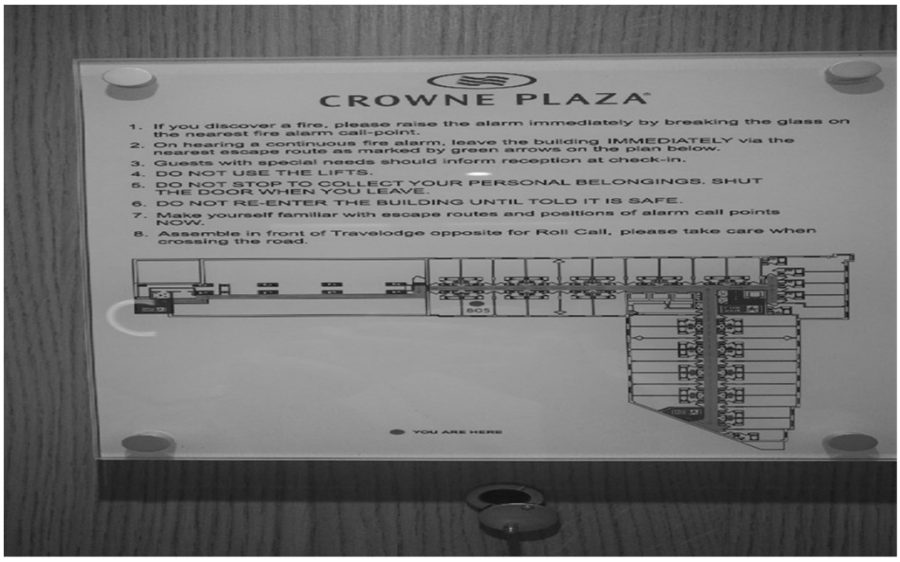
Advanced Learning from the Latest Data Breach Incidents

Jonathan Armstrong

0

Have a Plan



@CorderyUK

1

Have a Plan

- Breaches are inevitable – think when not if
- KISS
- Make sure people are trained on the plan – think fire drill
- Understand human dynamics
- Rehearse

@CorderyUK

2

Know your Data and your Third Parties

@CorderyUK

3

Know your Data and your Third Parties

- Disaggregated world
- Do due diligence (e.g. payroll provider)
- Do proper contracts (inc. intra-group e.g. Equifax)
- Make sure you address data transfer (death of SCCs + safe harbor?)
- Do proper acquisition due diligence too (e.g. Marriott/Starwood)

4

Know your Data and your Third Parties

"Multinational data companies like Equifax must understand what personal data they hold and take robust steps to protect it. Their boards need to ensure that internal controls and systems work effectively to meet legal requirements and customers' expectations"

Elizabeth Denham

5

Assemble your Team

6

Assemble your Team (cont'd)

- Make sure compliance has a seat at the table
- Look at the technical skills you will need
- Consider PR rapid response
- Watch your share/stock price
- Do due diligence on the team (e.g. Morrisons)
- Rehearse and understand culture (e.g. Germany)

7

DPIA Everything

8

DPIA Everything

- Look creatively at risk
- Make sure those responsible for the process own the DPIA
- Credit for math

9

Do SARs and DSRs real good

10

Do SARs and DSRs real good

- Often a sign of pain
- Can be used as advanced early warning
- DPAs investigate SARs & DSRs too (eg Met Police; Cambridge Analytica)

11

Respect the Time

@CorderyUK

12

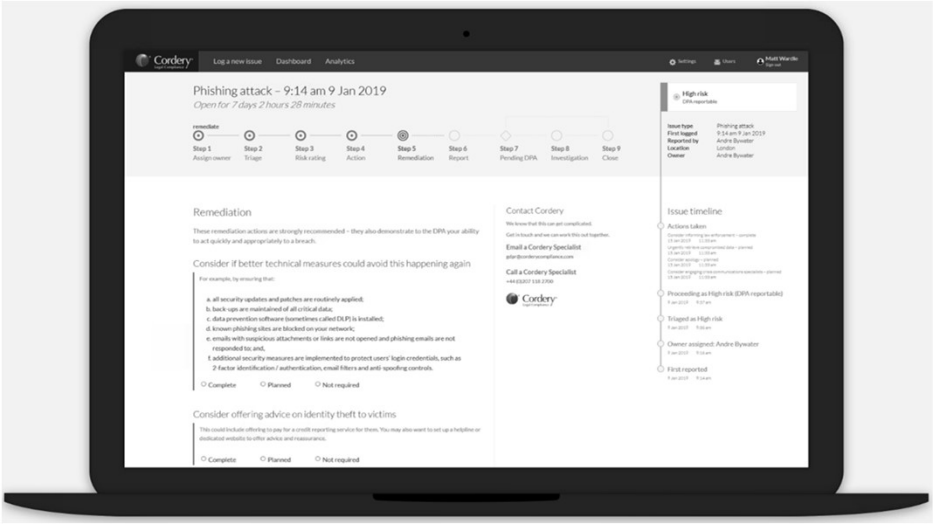
Respect the Time

- TalkTalk
- 'good curry test'

@CorderyUK

13

Remediate then Report



Remediate then Report

- Show you've learnt lessons
- Look at prior regulatory interventions
- 'Do the right thing'
- Don't try and chip victims (e.g. new contractual terms)
- Look for the simple too (e.g. padlocks)
- Do the easy now (e.g. patch management; training)

Don’t diss the DPA

16

Don’t diss the DPA

- TalkTalk
- Cambridge Analytica
  - Carroll had no more right to submit a SAR “*than a member of the Taliban sitting in a cave in Afghanistan*”
  - SCL did “*not expect to be further harassed with this sort of correspondence*”
- It’s not just about the breach –
  - Look at the other 5 principles especially transparency (false promises are common e.g. BA; Equifax) and lawful transfer

17

Keep Logs

18

Keep logs

- You need a record of all incidents
- DPAs are asking to see data breach logs
- Breaches may need to be disclosed if you get a SAR

19

Debrief & Learn

@CorderyUK

20

Debrief & Learn

- Its never over until...
- Make sure you learn from every incident – reported or not

@CorderyUK

21

Resources

GDPR FAQs – www.bit.ly/gdprfaqs

GDPR Glossary – www.bit.ly/gdprwords

ICO Secures Criminal Convictions in Cambridge Analytica Subject Access Case- http://www.corderycompliance.com/ico-secures-criminal-convictions-against-ca-in-sar-case-2/

Breach Navigator - https://www.corderycompliance.com/lexisnexis-launches-cordery-breach-navigator/

Marriott - http://www.corderycompliance.com/ico-intention-to-fine-marriot-99-million-for-data-breach/

BA - http://www.corderycompliance.com/uk-dpa-to-fine-ba-for-data-breach/

Equifax - https://www.corderycompliance.com/equifax-fined-by-uk-data-protection-regulator-2/

Hilton 2017 Settlement - https://www.corderycompliance.com/client-alert-hilton-settles-us-data-breach-action/

@CorderyUK

22

Questions

Jonathan Armstrong
Partner
Cordery
T +44 (0)20 7075 1784
E jonathan.armstrong@corderycompliance.com
@armstrongjp

@CorderyUK

23