CITY
UNIVERSITY OF LONDON
EST 1894

# A triage playbook: privacy harm assessment and personal data breach incident response in the UK

Cher Devey

**MPhil/PhD Transfer Seminar**

20th March 2017

# Agenda

Motivation

Aim of this study

Research Questions

Approach

Findings & Summary

Future work & plan

Q&A

# Organisations & Data Privacy

Motivation

- Data privacy issues require **organisations** to re-examine the **data privacy** perspectives of the various parties, & the **ethical aspects** of the inter-relationship exchanges (Bonner 2012).

- The General Data Protection Regulation (GDPR): Data Protection Act 1998 (DPA) in May 2018.

- Data breaches are a reality.

‘***Data breach: any incident*** *involving* ***the loss or exposure of digital personal records***’ (Howard & Gulyas 2014).

# TalkTalk Data Breach & GDPR

Motivation

TalkTalk (UK ISP/Telco) **data breach** (Oct. 2015):

❖156,959 customers details; Government inquiries;

❖CEO resigned;

❖**£400k fine** by Information Commissioner's Office (ICO).

Under the GDPR:

❖TalkTalk could have been fined over £70 million;

❖Mandatory **breach notification**; likely ***consequences*** of personal data breach i.e. **the privacy harm to individuals;**

❖Data subjects: rights to **claim compensation**.

'Distress' (a **privacy harm**) is a 'damage' under DPA

***What is 'distress'*** *?*

# TalkTalk DBI Response & Consequences

A TalkTalk customer was “**fuming”** after **being on hold** to TalkTalk customer services **for more than an hour.** Her remarks:

*‘I’m **very concerned** that my bank details may have been taken but didn’t want to have to change **all bank details**. It’s a lot of hassle doing so but now it looks like I will have to after the disgusting customer service’.*

*‘I **was angry** enough being on hold that long but to then **be cut off is terrible**… the **timing of the announcement** was “**not really acceptable**”’.*

*‘The **late announcement** is **not really acceptable** either but **even worse is the communications.** By the time people are informed who knows how much could have been stolen’.*

**(www.theGuardian.com, 2015)**

# Aim of this study

To develop a corporate personal data breach incident response *playbook* that organisations can use in the initial stages of an incident response, so that privacy harm is minimised.

*A playbook refers to a set of scripts (scripts for action) for conducting the response activities.*

# Research Questions (RQ)

a) *What constitutes a **personal data breach incident (DBI)**?*

b) *What are the characteristics of existing **incident response** frameworks?*

c) *What is **triage** & how does it work?*

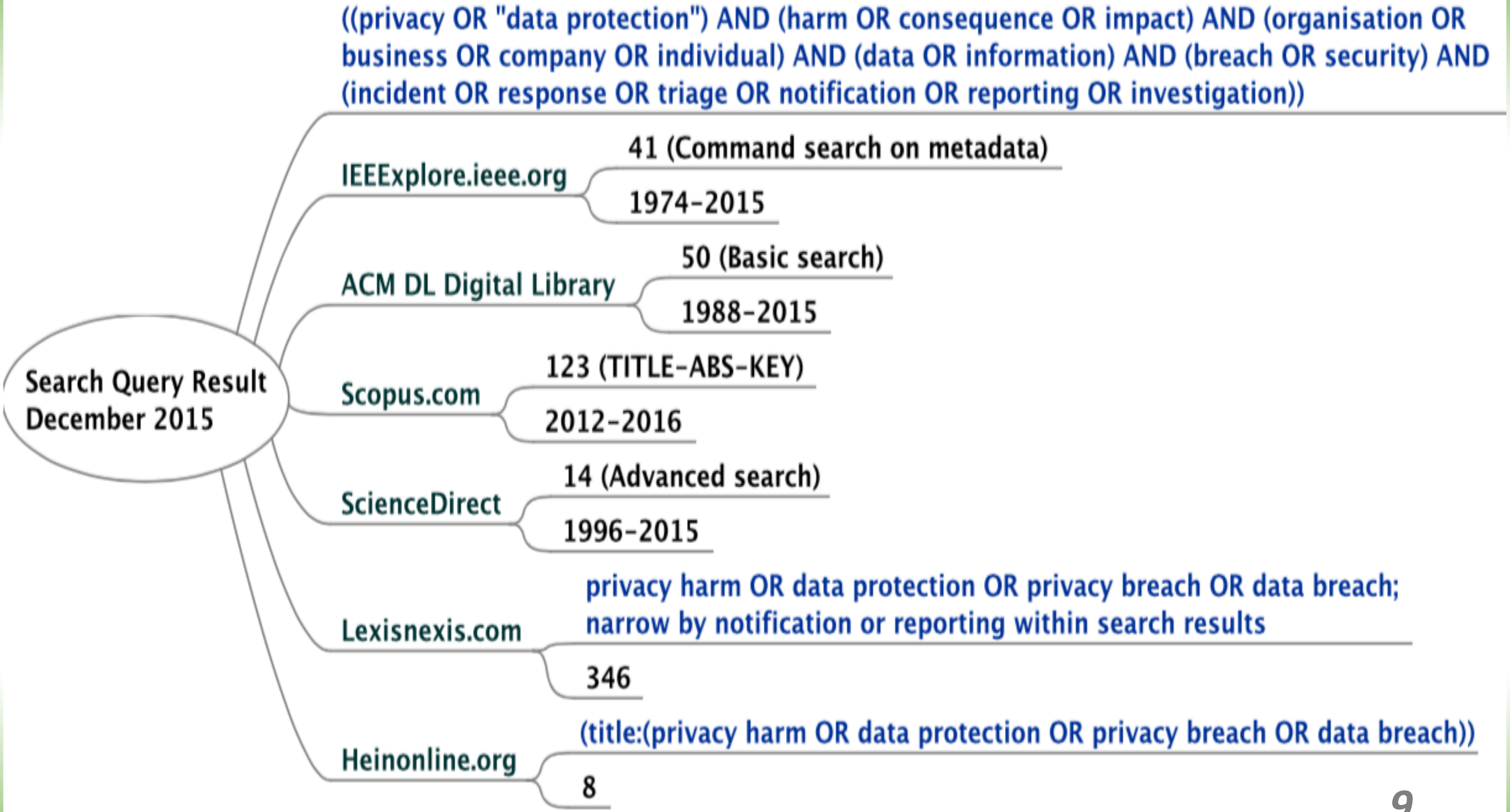
# Systematic Scoping/Mapping Studies(SSM)

**Structured approach:** literature search & review; **synthesis of collected literature**.

**Explore** a given topic: **little evidence available;** & **guide a future further studies** (Barreiros 2011).

- ✪IEEE Xplore, ACM & Scopus (Dybå et al. 2007) & (Kitchenham & Brereton 2013).
- ✪ScienceDirect, WestLaw, LexisNexis, Hein, ENISA.europa.eu, ICO.org.uk, SEI-CMU, CERT.org, Google Scholars, EThOS, Academia.net, Researchgate.net.
- ✪Events & conferences.

SSM based on Petersen et al. (2008).



Search Query Result December 2015

((privacy OR "data protection") AND (harm OR consequence OR impact) AND (organisation OR business OR company OR individual) AND (data OR information) AND (breach OR security) AND (incident OR response OR triage OR notification OR reporting OR investigation))

IEEExplore.ieee.org
- 41 (Command search on metadata)
- 1974-2015

ACM DL Digital Library
- 50 (Basic search)
- 1988-2015

Scopus.com
- 123 (TITLE-ABS-KEY)
- 2012-2016

ScienceDirect
- 14 (Advanced search)
- 1996-2015

Lexisnexis.com
- privacy harm OR data protection OR privacy breach OR data breach; narrow by notification or reporting within search results
- 346

Heinonline.org
- (title:(privacy harm OR data protection OR privacy breach OR data breach))
- 8

# Personal Data & Data Breach

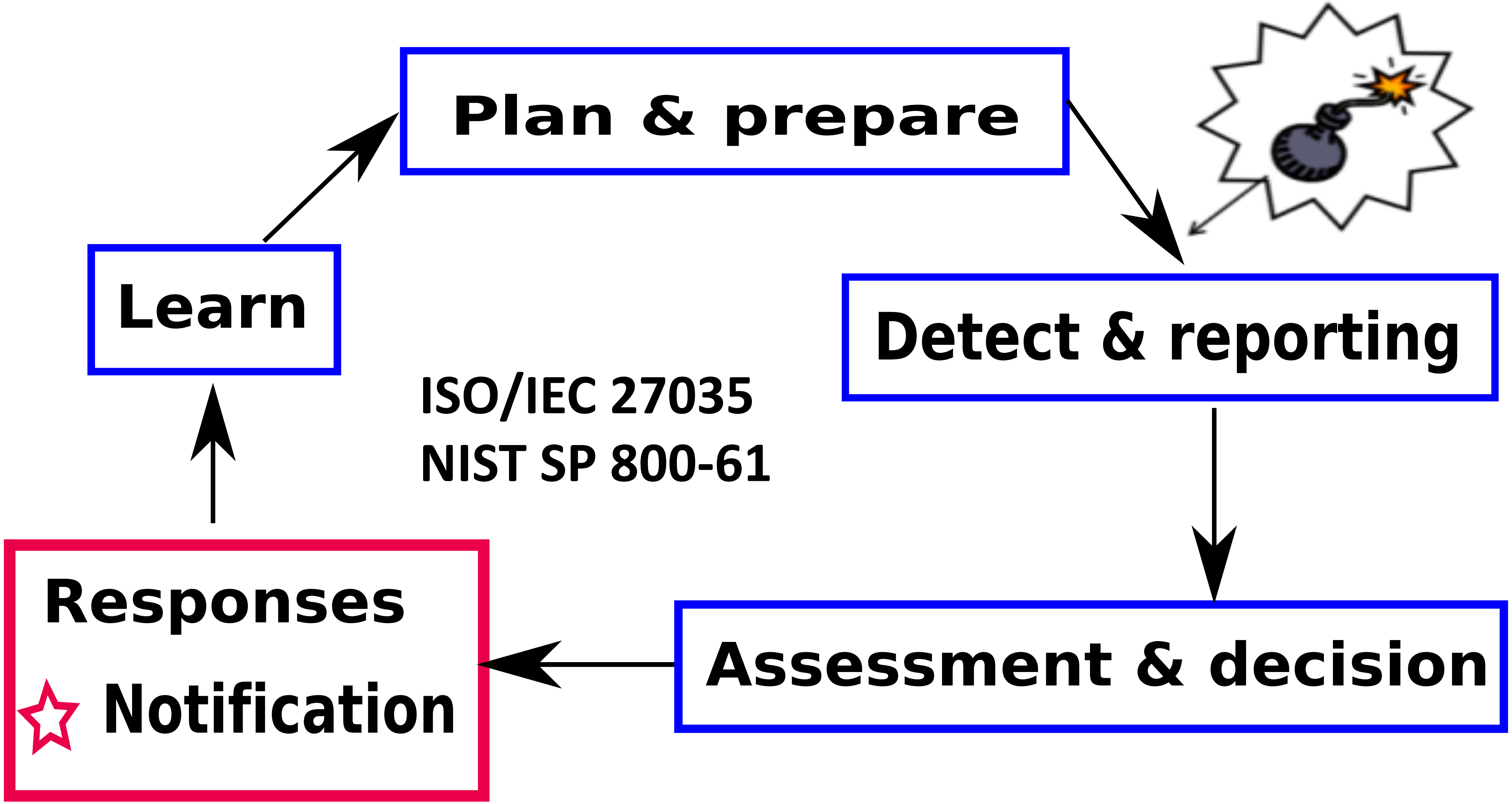
RQ a)

- ***‘Personal records*** *are defined as a) data containing* ***privileged information*** *about an individual that cannot be readily obtained through other public means & b) this information only known by an individual or by an organisation under* ***the terms of a confidentiality agreement’*** (Howard and Gulyas 2014).
- ***‘Personal data breach*** *means* ***a breach of security leading to the …’*** (GDPR).
- *‘A personal data breach can be the* ***result of a security incident,*** *but also of loss of user control.* ***An information security incident does not necessarily entail a personal data breach & vice versa’*** (ENISA 2012).

- **Personal data breach or data breach – the breach (DB)**
- **DB incident (DBI)**

RQ b)

# Incident Management Process (IMP Lifecycle) (Tøndel et al. 2014)

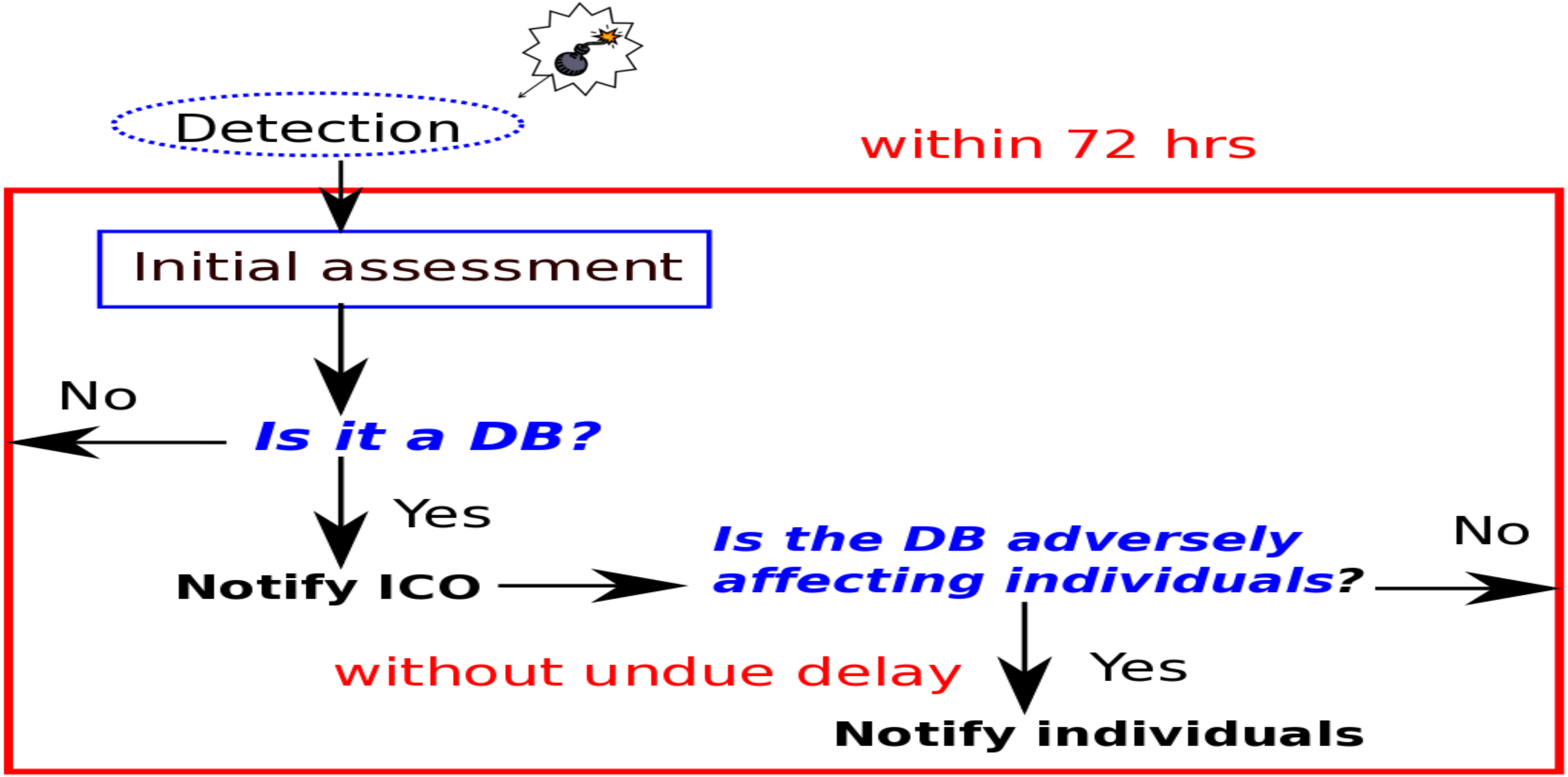


ISO/IEC 27035
NIST SP 800-61

# ✪DB handling procedure (ENISA 2012)

RQ a),b)

✪Data breach notification: complex; **nature of the breach**



Detection

within 72 hrs

Initial assessment

No

Is it a DB?

Yes

Notify ICO

Is the DB adversely affecting individuals?

No

without undue delay

Yes

Notify individuals

# Incident & DBI Response

RQ a),b)

- ✰**Personal data breach incident (DBI) response: not yet been extensively researched** as a topic.
- ✰Impact assessments: **privacy harm** or **avoiding harm to people** in incident response **not yet been extensively researched.**
- ✰Data-breach scenarios: **nuanced, complex, diverse scenarios**; **difficulty in making good policies** (Howard & Gulyas 2014 ).
- ✰**Security incident management standard,** ISO/IEC 27035:2011 & **triage approach** from ENISA (2010) used by Hove & Tårnes (2013).
- ✰An incident management ontology **(+ incident triage)**; **not yet been applied to a real world** individual/organisation (Mundie et al. 2014).

# Incident Triage

RQ c)

- ✪Triage for **DBI response has not been extensively researched.**
- ✪**ONE** computer forensics triage model by Rogers et al. (2006): **within the first few hours of an investigation**; for suspect investigation**;** on-site **analysis of computer system(s**).
- ✪Incident triage under **incident response** (Brownlee & Guttman 1998):
  - ❖Investigating whether **indeed an incident occurred**.
  - ❖Determining the **extent of the incident.**

*'Triage is an area in which decision makers must know what they are doing, why they are doing it, & **which actions to take** to achieve a satisfactory outcome'* (Moser & Cohen 2013).

# Call for Further Research Directions

- ✫Future research directions should strive to better **understand business challenges** related to the **impact caused by incidents** (Silic & Back 2014).

- ✫In addressing the **human aspect of information security,** Metalidou et al. (2014) stress that human factors have not been given enough attention in the literature.

- ✫‘*Incident response starts with* ***people to take the necessary actions,*** *& this decade is one of* ***response***’ (Schneier 2014).

**Little research on DBI response, incident triage & privacy *harm* to individuals**

# DBI Interviews Study Objectives

- ✪ *What frameworks/procedures/processes are being used for DBI response?*
- ✪ *What are the DBI response activities or processes?*
- ✪ *What are the concerns or views on the DBI activities, on notification to individuals, & on privacy harm affecting individuals?*

# DBI Interview Study

- ✪**Qualitative semi-structured** interview.
- ✪Participants given: brief notes; a consent form; last not more than **one hour, audio-recorded** & conducted face-to-face.
- ✪**Twenty-one** practitioners: **relevant job titles** or work experiences; **across industry sectors.**
- ✪**Face-to-face** between 23-May-2016 to 19-July-2016.
- ✪Recorded interviews: **transcribed**, analysed & reported using **Hybrid Thematic Analysis** (Willig 2013) & **Explanatory Approach** **(**Willig 2013), (Ritchie et al. 2014) & (Fereday & Muir-Cochrane 2006).

# Hybrid Thematic Analysis Steps

1. Set up coding approaches;
2. **Pre-coded** questions (**topics**);
3. Create participants’ map with topics;
4. Code & extract text from transcribed files into participants’ map, 'broad' & 'recurrent' theme maps (**1st pass coding**);
5. Extract themes created during **1st pass coding** into ‘consolidated’ theme maps (**2nd pass coding**);
6. Final analysis & reporting of themes (**Explanatory Approach: 3 Questions; EQ1, EQ2, EQ3**).

***What did the interviews expose?***

# *EQ1 What frameworks are being used for DBI response?*

**No dedicated framework** for handling DBI response. Various approaches:

- **Crisis management framework:** for all incidents;
- **Multiple procedures:** *'We also need to fine tune the controls to ensure we meet the various requirements for the **GDPR**'* (F16);
- **No formal written procedures:** *'**Ad hoc**, so it was called into existence at the moment that we were notified'* (O20).
- ***'Why have a framework if you know you can't do the first step - value the piece of data?'*** (F21).

# IMP Lifecycle (Tøndel et al. 2014) & standards/guidelines

- ✰‘*Quite simplistic* - does *not handle spectrum of cases in hospital’* (H5).
- ✰‘*In reality it is “wishy washy”’* (L19).
- ✰‘*Getting a good working set of standards was difficult’* (C18).
- ✰The ISO/IEC 27035:2011 **not used;** information security management process or policy have been adopted.
- ✰ENISA’s (2012) **DBI handling procedure** was not mentioned or used.
- ✰ICO breach management plan - **not appropriate** during DBI response **as time was of essence**.
- ✰Standards or industry driven frameworks: **expensive; for ‘tick box’ & not taken seriously.**

# *EQ2 What are the concerns/views on DBI response activities?*

- No objection on the **notification** to individuals.
- **Each breach is different**; Unlikely to capture all the **nuances of incident response.**
- *‘People will take some time to get used to - to understand - what the breach is’* (H7).
- *‘Should be able to just spot it right there to **say it is personal data**’ (E6).*
- *‘Work on a situation that you know it’s breached’ (F12).*

# Accurate information & timely response

At the initial phase, **actionable information** or ‘something has been lost/corrupted/stolen’ or **accurate information** was usually **not readily available.**

- ✮*‘The response **should be immediate** to actually make customers aware that their data may have been compromised, **even if it has not’*** (B3).
- ✮*‘The **response framework is far too slow.**, even if it was unintentional, ...the **victim has to continually suffer the consequences of that’*** (F4).

# Views on the TalkTalk DBI response

- ‘The CEO communicated with the press ‘*before she actually had **a real handle on the problem**’ (B13).*

- *‘It must have been **horrendous situations** for large organisations like TalkTalk **to respond in such a short timeframe (GDPR)**’ (F12).*

- *‘If we are **ethical** we should be doing things in line with **what is right** & in **the spirit of the law**’* (B13).

**Avoid the TalkTalk DBI response.**

## *EQ3 What are the concerns/views on privacy harm to individuals?*

- ***‘Information means different things to different people’*** (B9).
- *‘If they breach confidence* ***they don’t think data breach is important even though privacy is a human right’*** (H7).
- ‘*Where* ***privacy & security don’t talk to each other: an organisation has got to really review its governance’*** (B11).
- ‘*Most people, most* ***organisations will look at harm*** *through* ***the lens of harm to the organisation***’ (B11).
- DBI (fraud): **nuisance, annoyance; immense disruption to professional & personal life.**
- DBI (email phishing): **distressed** members; *‘Mr. Angry’ emails;* **very angry, cross & absolutely furious; members resigned.**

# Organisations & DBI

RQ

Summary

- ✯DBI affects all organisations irrespective of sizes & industry sectors & DBI have not ceased.
- ✯DBI responses focusing on **the likely harm to individuals (privacy harm) will require new ways of thinking.**
- ✯Primary business goals: **profits making,** maintaining **reputation** also drives their **response posture** in terms of **prioritisation:** ***whether to or not to disclose/notify DBIs.***

***To minimise privacy harm - concerns for their customers should drive the DBI response.***

# Use of Questions in Triage for DBI Response

RQ a),b)

S
u
m
m
a
r
y

- ✫**Use of questions resembling a checklist of steps** during triage.
- ✫***Nature of the breach*** would **change the types of questions** which then **lead to actionable information**.
- ✫***Is it a DB***? : ‘***assumed you’re breached***’ & ‘***err on the side of your customers***’.
- ✫Work towards an **actionable, proportionate & ethical response** that **minimises the harm to your customers.**
- ✫To have a **handle on the nature of the breach** such that **affected individuals were alerted to the problem.**

# DBI Response Activities - Synthesised from Interviews

RQ b),c)

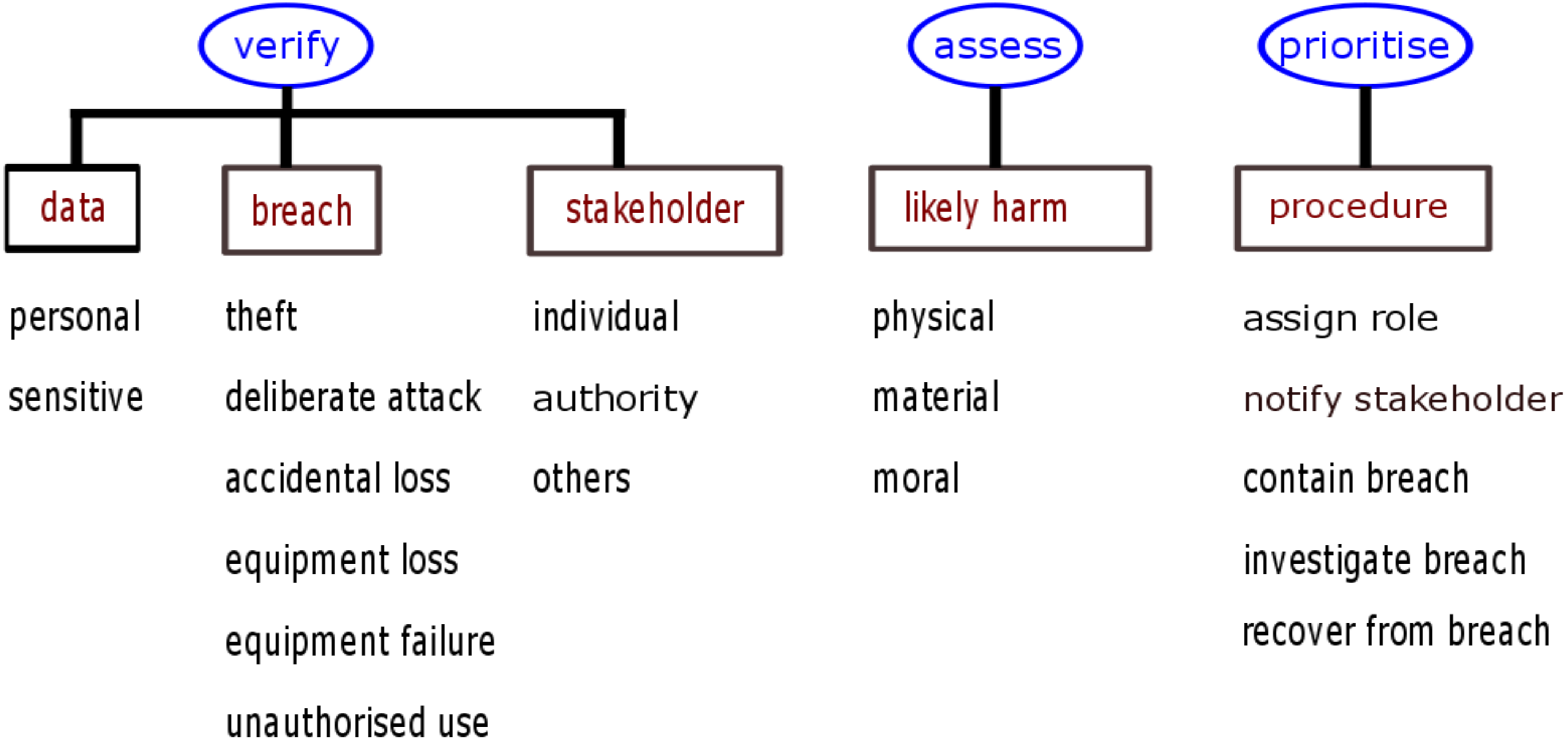
S
u
m
m
a
r
y

- pre-response
  - communication plan
  - training
  - team roles
- *incident detected/reported*
- **triage**
  - **gather & assess**
  - **privacy harm assessment (PHA)**
- notify
- investigate
- subsequent response
- recover/remediate

✫Outcome of triage: **obtain actionable information**.

# Triage for DBI Response

RQ c)



verify

- data
  - personal
  - sensitive
- breach
  - theft
  - deliberate attack
  - accidental loss
  - equipment loss
  - equipment failure
  - unauthorised use
- stakeholder
  - individual
  - authority
  - others

assess

- likely harm
  - physical
  - material
  - moral

prioritise

- procedure
  - assign role
  - notify stakeholder
  - contain breach
  - investigate breach
  - recover from breach

## Triage Entities - Synthesised From Literature

# Privacy harm

RQ

**Summary**

- ✭Privacy harm: *tricky to measure;* ***value* attached to personal data (*Human costs*).**
- ✭Privacy & ethics: important; privacy is **all ethics-based.**
- ✭The *genie was out of the bottle* out in the *wild* - **the harm was already done.**
- ✭**The triage for DBI response provides a way to minimise the harm. This requires privacy harm assessment (PHA) during triage.**

**Gap: a PHA approach in triage for DBI response.**

# Future Work Aim

Overall aim: ***a triage - PHA playbook for organisations in the UK (A triage playbook).***

Outcome of using the **triage playbook** for **DBI response to individuals** is to **minimise the privacy harm**.

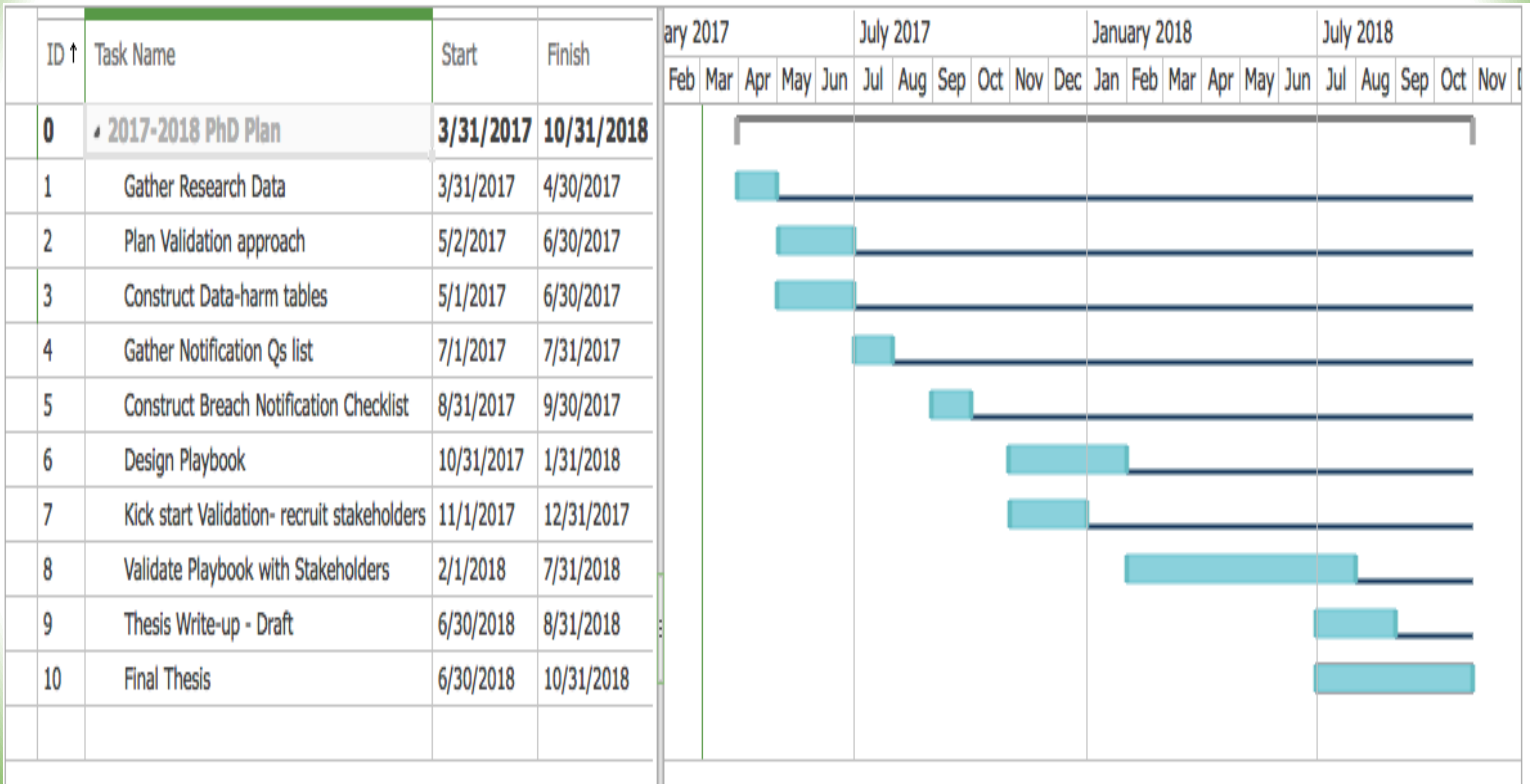
**Triage playbook** characteristics:

❖applicable for use during **initial DBI response**;

❖enable **nature of the breach** & **privacy harm** to be assessed (PHA) for **timely** DBI response to **individuals**;

❖enable **ethical, proportionate** responses to individuals such that the **harm to individuals are minimised**.

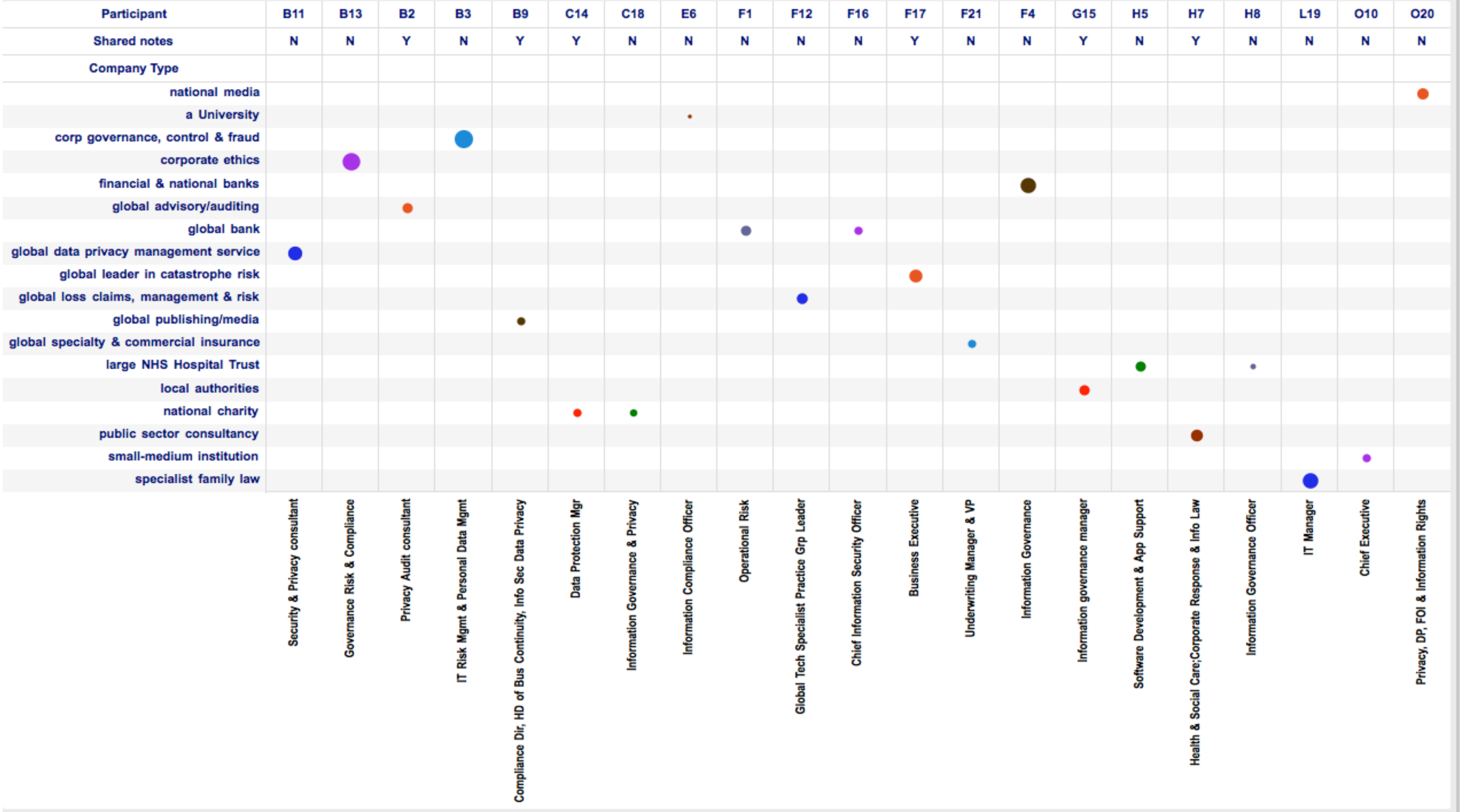
# Future Work Plan



| ID ↑ | Task Name | Start | Finish |
|---|---|---|---|
| **0** | **2017-2018 PhD Plan** | **3/31/2017** | **10/31/2018** |
| 1 | Gather Research Data | 3/31/2017 | 4/30/2017 |
| 2 | Plan Validation approach | 5/2/2017 | 6/30/2017 |
| 3 | Construct Data-harm tables | 5/1/2017 | 6/30/2017 |
| 4 | Gather Notification Qs list | 7/1/2017 | 7/31/2017 |
| 5 | Construct Breach Notification Checklist | 8/31/2017 | 9/30/2017 |
| 6 | Design Playbook | 10/31/2017 | 1/31/2018 |
| 7 | Kick start Validation- recruit stakeholders | 11/1/2017 | 12/31/2017 |
| 8 | Validate Playbook with Stakeholders | 2/1/2018 | 7/31/2018 |
| 9 | Thesis Write-up - Draft | 6/30/2018 | 8/31/2018 |
| 10 | Final Thesis | 6/30/2018 | 10/31/2018 |

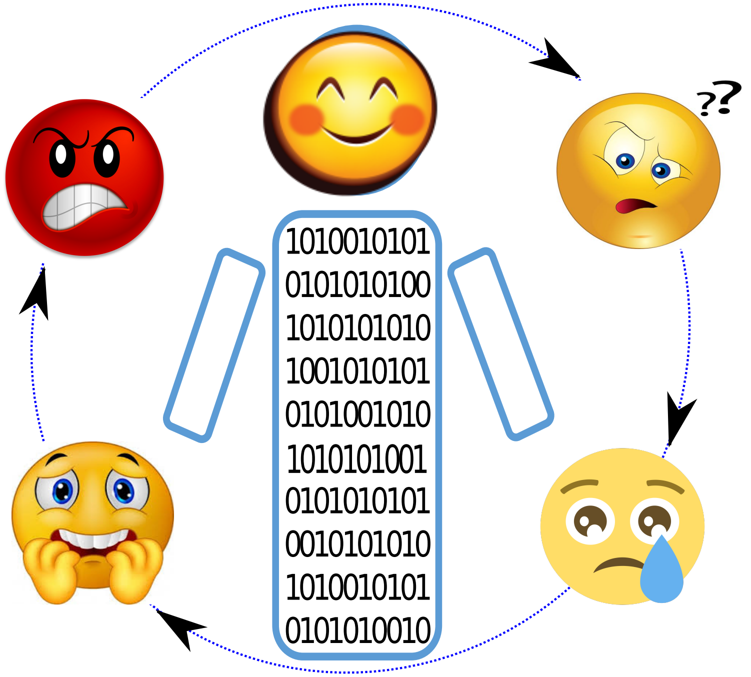
# Q&A

# Thank You.



| Participant | B11 | B13 | B2 | B3 | B9 | C14 | C18 | E6 | F1 | F12 | F16 | F17 | F21 | F4 | G15 | H5 | H7 | H8 | L19 | O10 | O20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Shared notes | N | N | Y | N | Y | Y | N | N | N | N | N | Y | N | N | Y | N | Y | N | N | N | N |
| Company Type | | | | | | | | | | | | | | | | | | | | | |
| national media | | | | | | | | | | | | | | | | | | | | | ● |
| a University | | | | | | | | ● | | | | | | | | | | | | | |
| corp governance, control & fraud | | | | ● | | | | | | | | | | | | | | | | | |
| corporate ethics | | ● | | | | | | | | | | | | | | | | | | | |
| financial & national banks | | | | | | | | | | | | | | ● | | | | | | | |
| global advisory/auditing | | | ● | | | | | | | | | | | | | | | | | | |
| global bank | | | | | | | | | ● | | ● | | | | | | | | | | |
| global data privacy management service | ● | | | | | | | | | | | | | | | | | | | | |
| global leader in catastrophe risk | | | | | | | | | | | | ● | | | | | | | | | |
| global loss claims, management & risk | | | | | | | | | | ● | | | | | | | | | | | |
| global publishing/media | | | | | ● | | | | | | | | | | | | | | | | |
| global specialty & commercial insurance | | | | | | | | | | | | | ● | | | | | | | | |
| large NHS Hospital Trust | | | | | | | | | | | | | | | | ● | | ● | | | |
| local authorities | | | | | | | | | | | | | | | ● | | | | | | |
| national charity | | | | | | ● | ● | | | | | | | | | | | | | | |
| public sector consultancy | | | | | | | | | | | | | | | | | ● | | | | |
| small-medium institution | | | | | | | | | | | | | | | | | | | | ● | |
| specialist family law | | | | | | | | | | | | | | | | | | | ● | | |
| | Security & Privacy consultant | Governance Risk & Compliance | Privacy Audit consultant | IT Risk Mgmt & Personal Data Mgmt | Compliance Dir, HD of Bus Continuity, Info Sec Data Privacy | Data Protection Mgr | Information Governance & Privacy | Information Compliance Officer | Operational Risk | Global Tech Specialist Practice Grp Leader | Chief Information Security Officer | Business Executive | Underwriting Manager & VP | Information Governance | Information governance manager | Software Development & App Support | Health & Social Care;Corporate Response & Info Law | Information Governance Officer | IT Manager | Chief Executive | Privacy, DP, FOI & Information Rights |

# Consequences of DBIs to victims



✯DBI (email phishing): **distressed** members; *'Mr. Angry' emails;* **very angry, cross & absolutely furious; resignation by members.**

✯DBI (fraud): **nuisance, annoyance; immense disruption to professional & personal life.**