Northumbria University
NEWCASTLE

Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection

James Nicholson, Lynne Coventry, Pam Briggs

PaCT Lab, Northumbria University

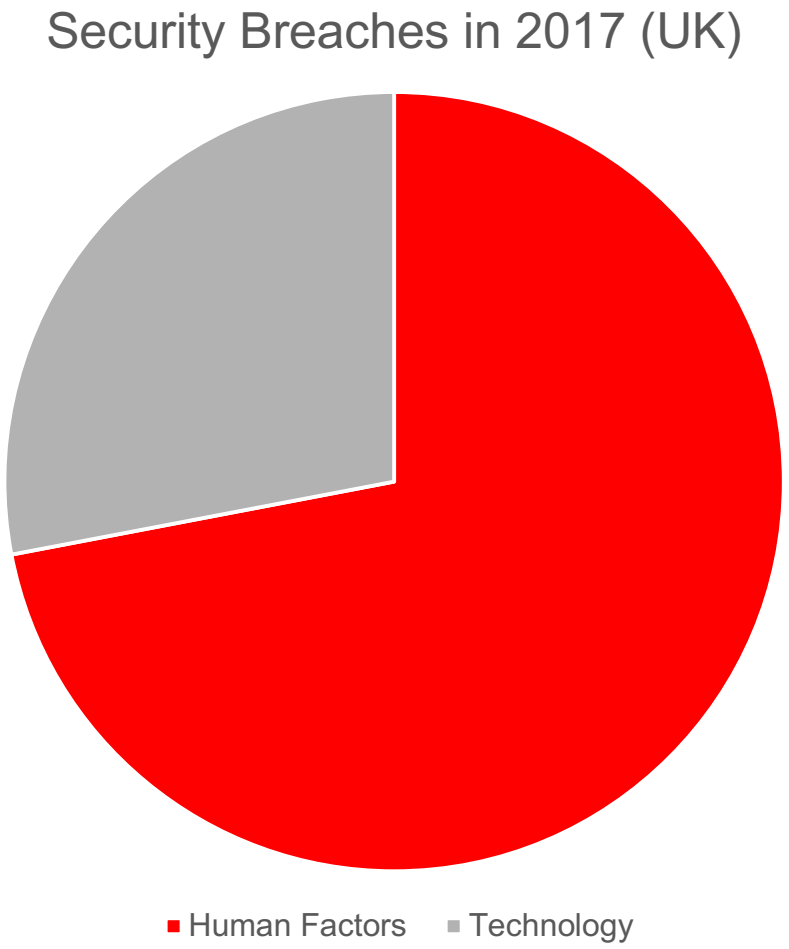
Newcastle, UK

Northumbria University NEWCASTLE

Background

Average cost of a cybersecurity breach:

-$3.5m



Kiahr, R., Shah, J.N., Sheriffs, P., Rossington, T., Pestell, G., Button, M. and Wang, V. *Cyber Security Breaches Survey 2017*.

Northumbria University NEWCASTLE

How do we assess an organisation's security culture?

- Self-report measurement tools:
  - SeBIS (16 self-reported items)
    - Device Securement, Password Generation, Proactive Awareness, Updating
      - e.g. "I do not change my passwords unless I have to." (Never => Always)
  - HAIS-Q (63 self-reported items)
    - Password management, Email use, Internet use, Social media use, Mobile devices, Information handling, Incident reporting
    - Knowledge / Attitude / Behaviour
      - E.g. "I share my work passwords with colleagues"

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873-2882). ACM.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*. 66, (May 2017), 40–51.

Wash, R., Rader, E. and Fennell, C. 2017. Can People Self-Report Security Accurately? *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17* (2017), 2228–2232.

Northumbria University NEWCASTLE

The Cybersurvival Task

- Purpose: Highlight cybersecurity misconceptions amongst employees and serve as a reflective exercise to security experts in organisation
- Expert = those responsible for setting the security agenda in their organisation
- Rank the 20 behaviours in order of importance for staying safe online in [organisation]

Item	My Ranking	Team Ranking	Answer	My Error	Team Error
1. Ask for advice			1		
2. Use strong passwords			9		
3. Use different passwords for accounts outside the organisation			3		
4. Do not disclose your personal password, even to the IT department			7		
5. Don't click on links from unknown senders			17		
6. Use antimalware software and keep it up to date			8		
7. Keep passwords safe if written down			4		
8. Save files to the network			2		
9. Report any data loss incidents			5		
10. Restrict physical access to computers and removable media			12		
11. Turn on automatic software updates			6		
12. Don't open attachments from unknown senders			15		
13. Educate yourself on how to avoid fraud			10		
14. Clear browser cookies			19		
15. Use additional authentication options (e.g. two-factor authentication)			11		
16. Don't open unnecessary attachments			16		
17. Look at the URL bar to verify you are visiting intended website			14		
18. Don't enter password when you click on a link in an email that takes you to a website that asks for the password			18		
19. Check if website you're visiting uses HTTPS			13		
Score					

Northumbria University NEWCASTLE

Overview of the Task

Stage	Approximate Duration
Generate List of Behaviours (Experts)	30 minutes
Workshops (Employees)	60 minutes (each)
Reflection (Experts)	45 minutes

Northumbria University NEWCASTLE

Generating the Behaviours

- Workshop with organisation's security experts
- Initial list of behaviours pre-compiled from Ion et al. (2015) and organisation's Information Security Policy
- Experts tasked with adding, removing, and rephrasing behaviours to reflect their desired focus for their organisation
- Experts asked to rank the final list of behaviours in order of importance for their staff to follow

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873-2882). ACM.

Ion, L., Reeder, R. and Consolvo, S. 2015. "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. *Symposium on Usable Privacy and Security* (2015), 327–346.

Northumbria University NEWCASTLE

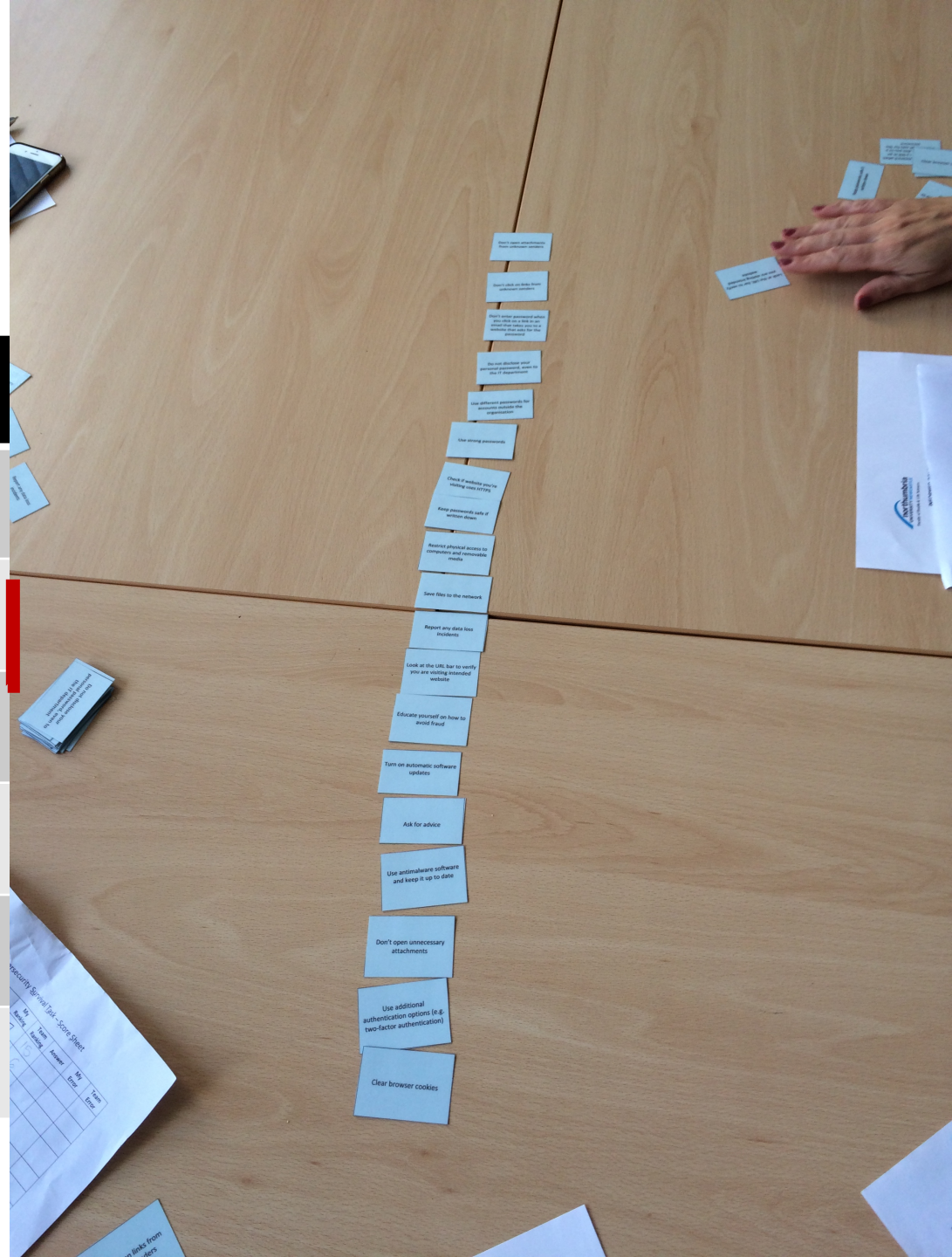
Employee Workshops

Activity	Approximate Duration
Introduction	2 minutes
Individual ranking of Cybersurvival Sheet	10 minutes
Reveal: top 3 and bottom 3 behaviours	10 minutes
Group ranking of Cybersurvival Sheet	25 minutes
Reveal of expert rankings	10 minutes
Debrief	3 minutes

Northumbria University NEWCASTLE

Employee Workshops

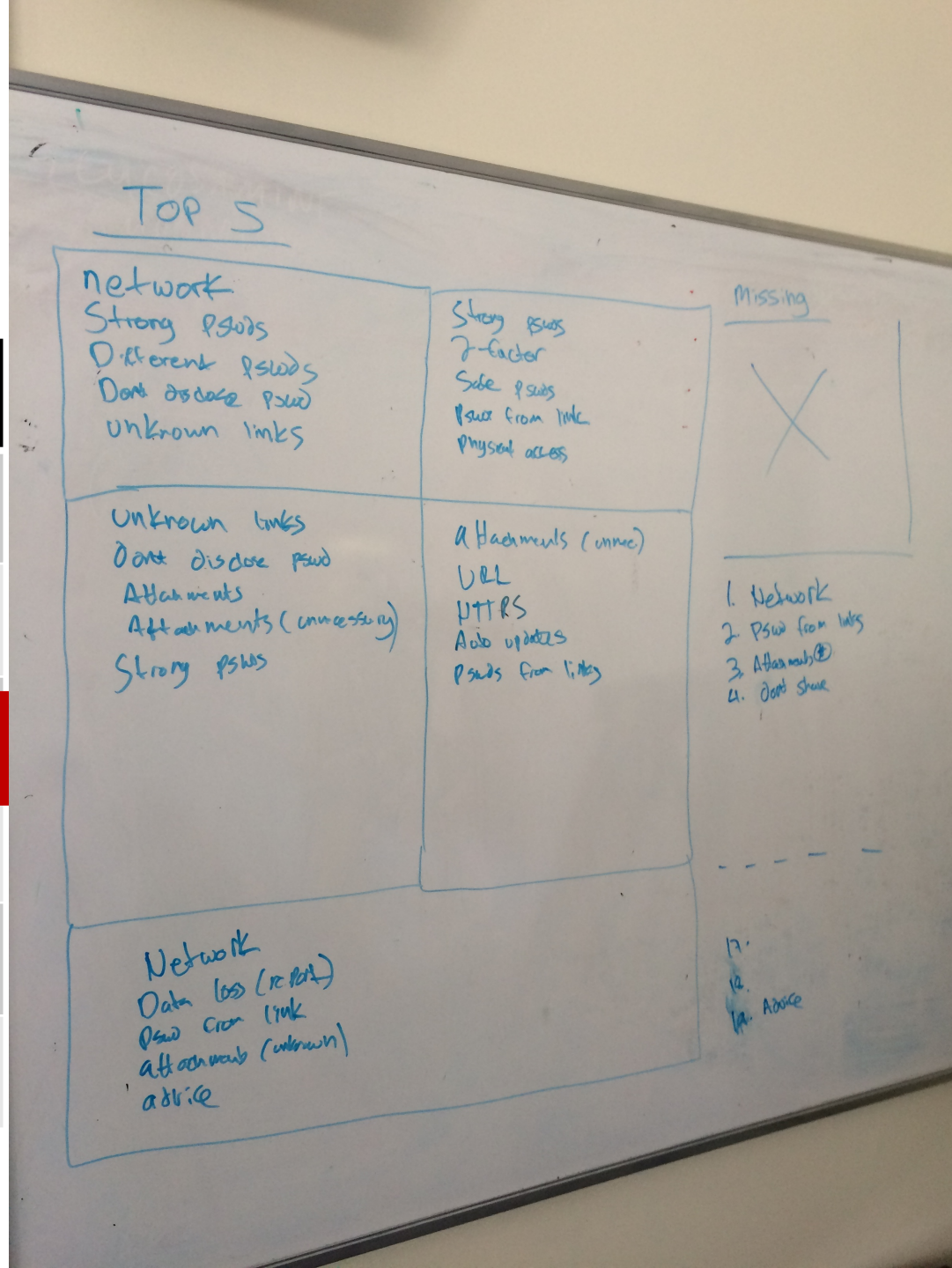
Activity	Approximate Duration
Introduction	2 minutes
Individual ranking of Cybersurvival Sheet	10 minutes
Reveal: top 3 and bottom 3 behaviours	10 minutes
Group ranking of Cybersurvival Sheet	25 minutes
Reveal of expert rankings	10 minutes
Debrief	3 minutes



Northumbria University NEWCASTLE

Employee Workshops

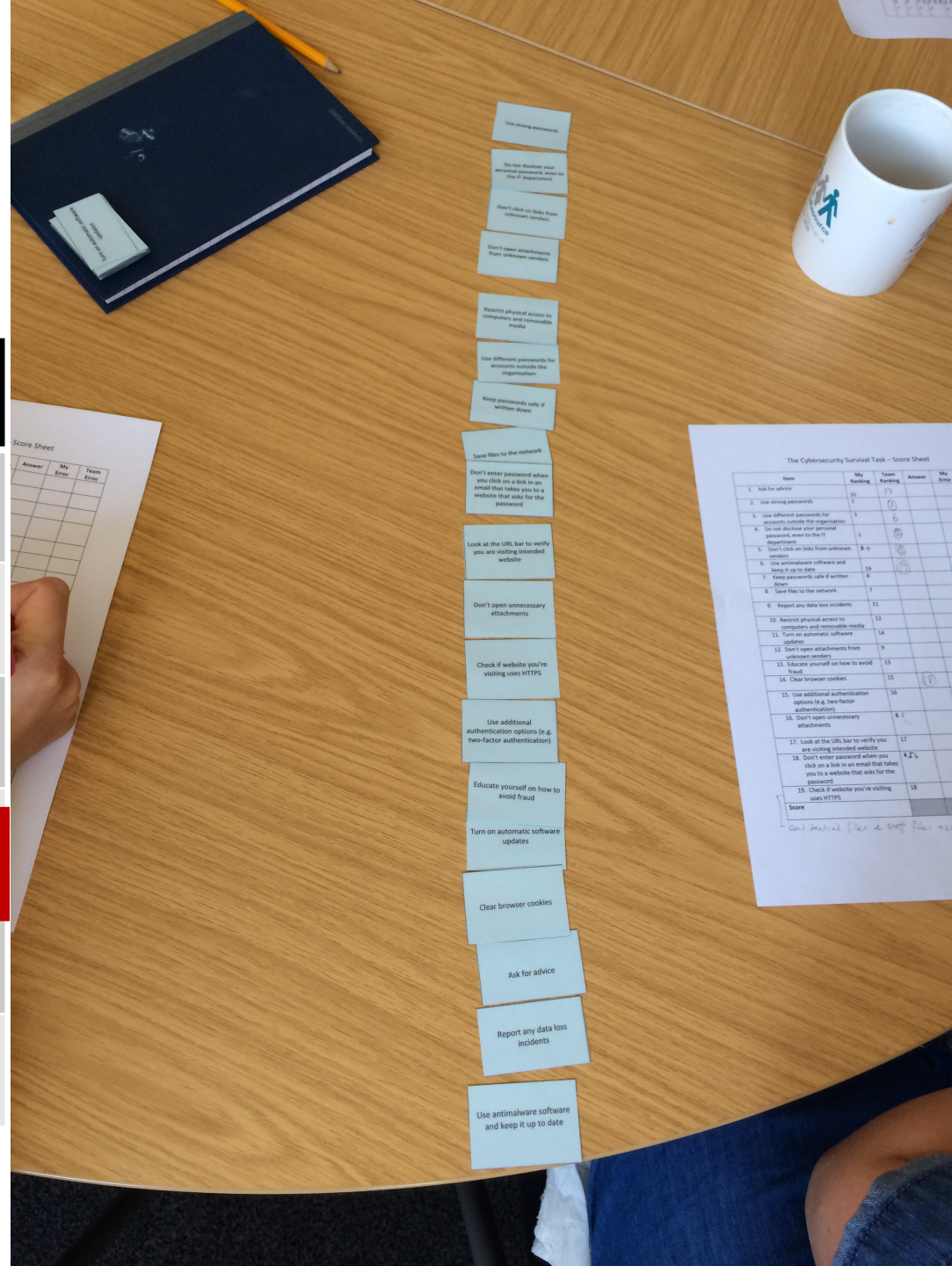
Activity	Approximate Duration
Introduction	2 minutes
Individual ranking of Cybersurvival Sheet	10 minutes
Reveal: top 3 and bottom 3 behaviours	10 minutes
Group ranking of Cybersurvival Sheet	25 minutes
Reveal of expert rankings	10 minutes
Debrief	3 minutes



Northumbria University NEWCASTLE

Employee Workshops

Activity	Approximate Duration
Introduction	2 minutes
Individual ranking of Cybersurvival Sheet	10 minutes
Reveal: top 3 and bottom 3 behaviours	10 minutes
Group ranking of Cybersurvival Sheet	25 minutes
Reveal of expert rankings	10 minutes
Debrief	3 minutes



Northumbria University NEWCASTLE

Employee Workshops

Activity	Approximate Duration
Introduction	2 minutes
Individual ranking of Cybersurvival Sheet	10 minutes
Reveal: top 3 and bottom 3 behaviours	10 minutes
Group ranking of Cybersurvival Sheet	25 minutes
Reveal of expert rankings	10 minutes
Debrief	3 minutes

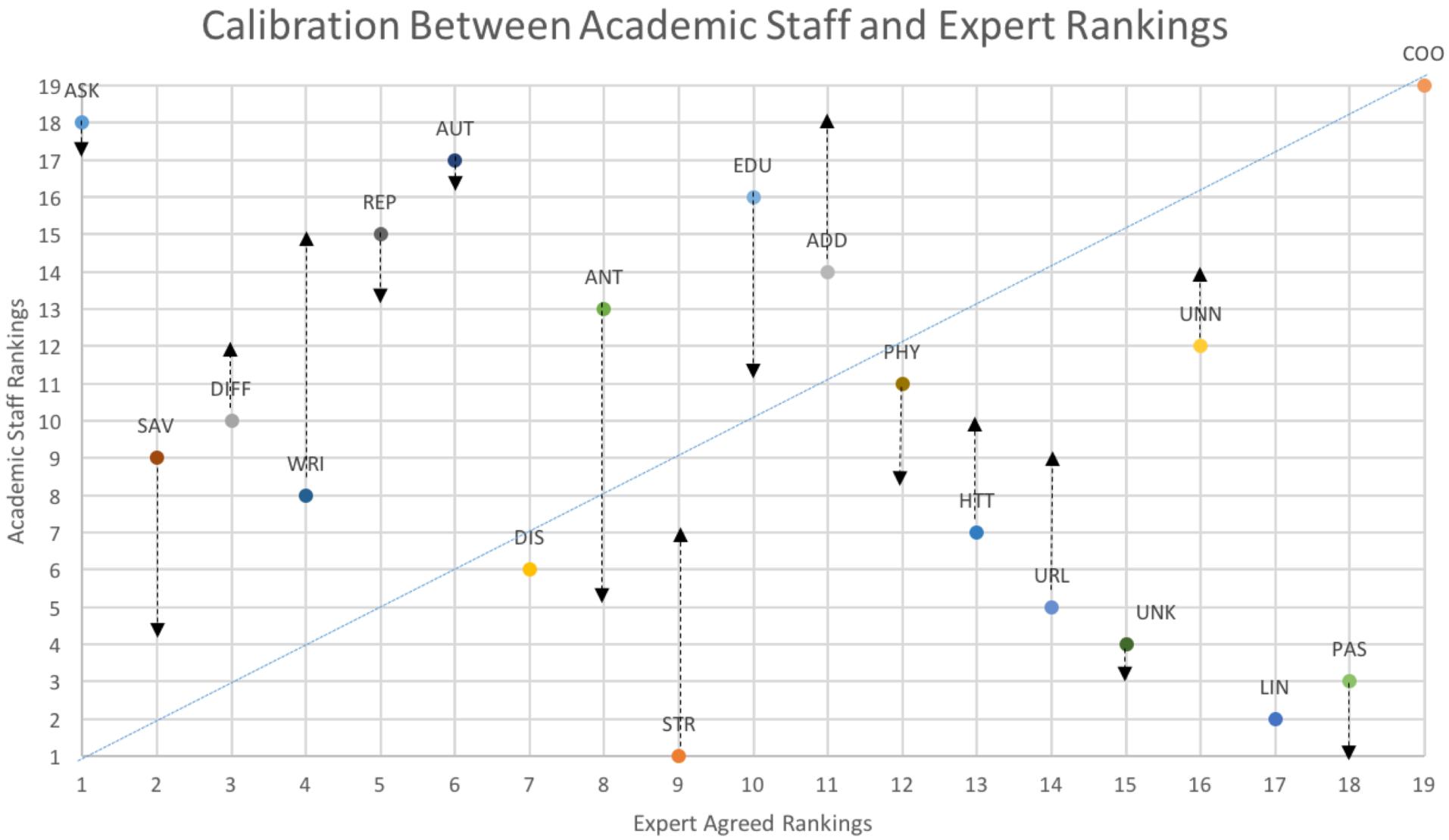
Northumbria University NEWCASTLE

Expert Reflection

- Experts presented with report highlighting:
  - Their rankings
  - Average employee rankings (individual and group)
    - Colour-coded highlighting of biggest shifts
  - Key reason for ranking of behaviour
- Experts alerted to biggest staff misconceptions

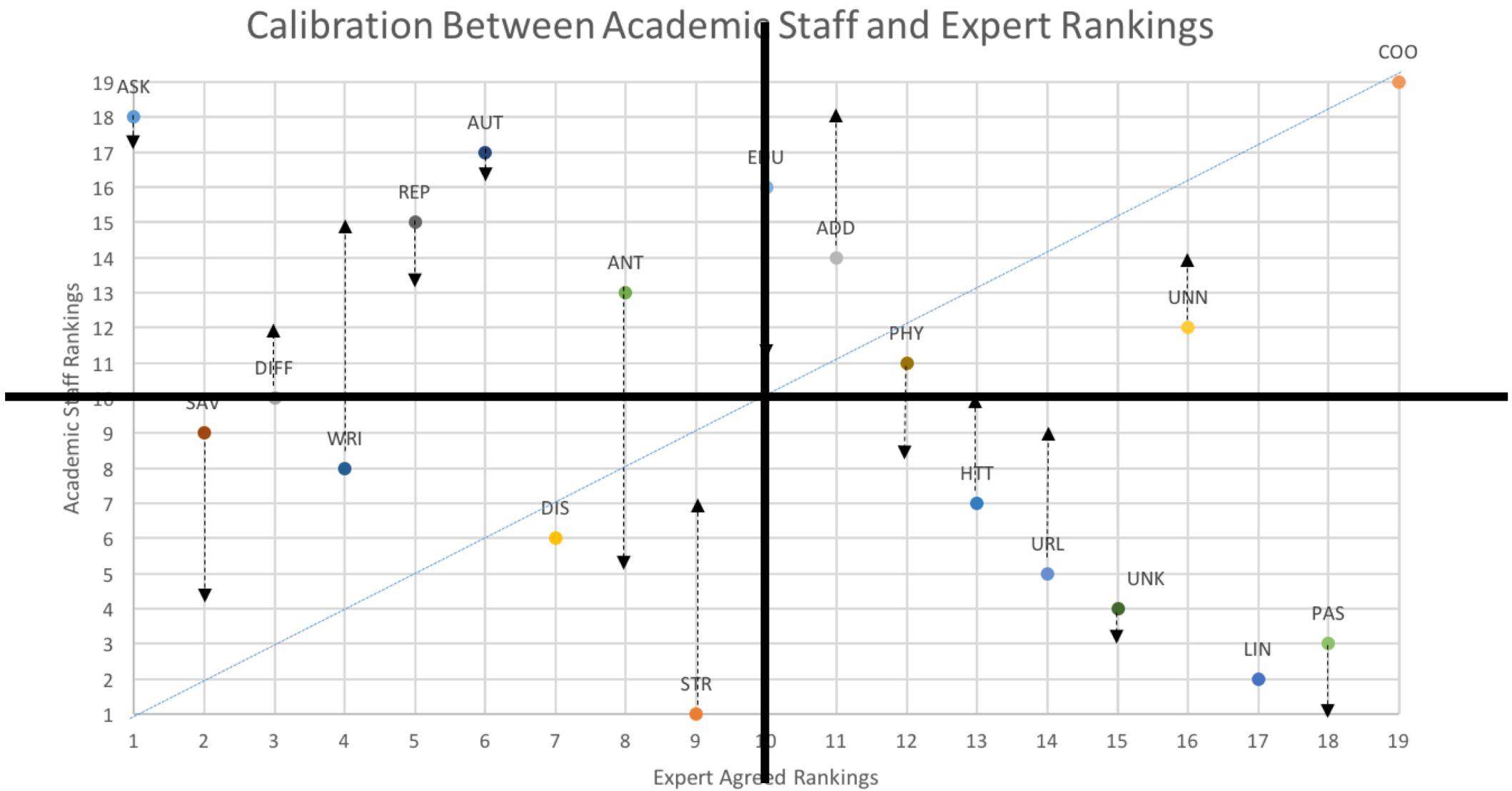
Northumbria University NEWCASTLE

Example Output: Discrepancies



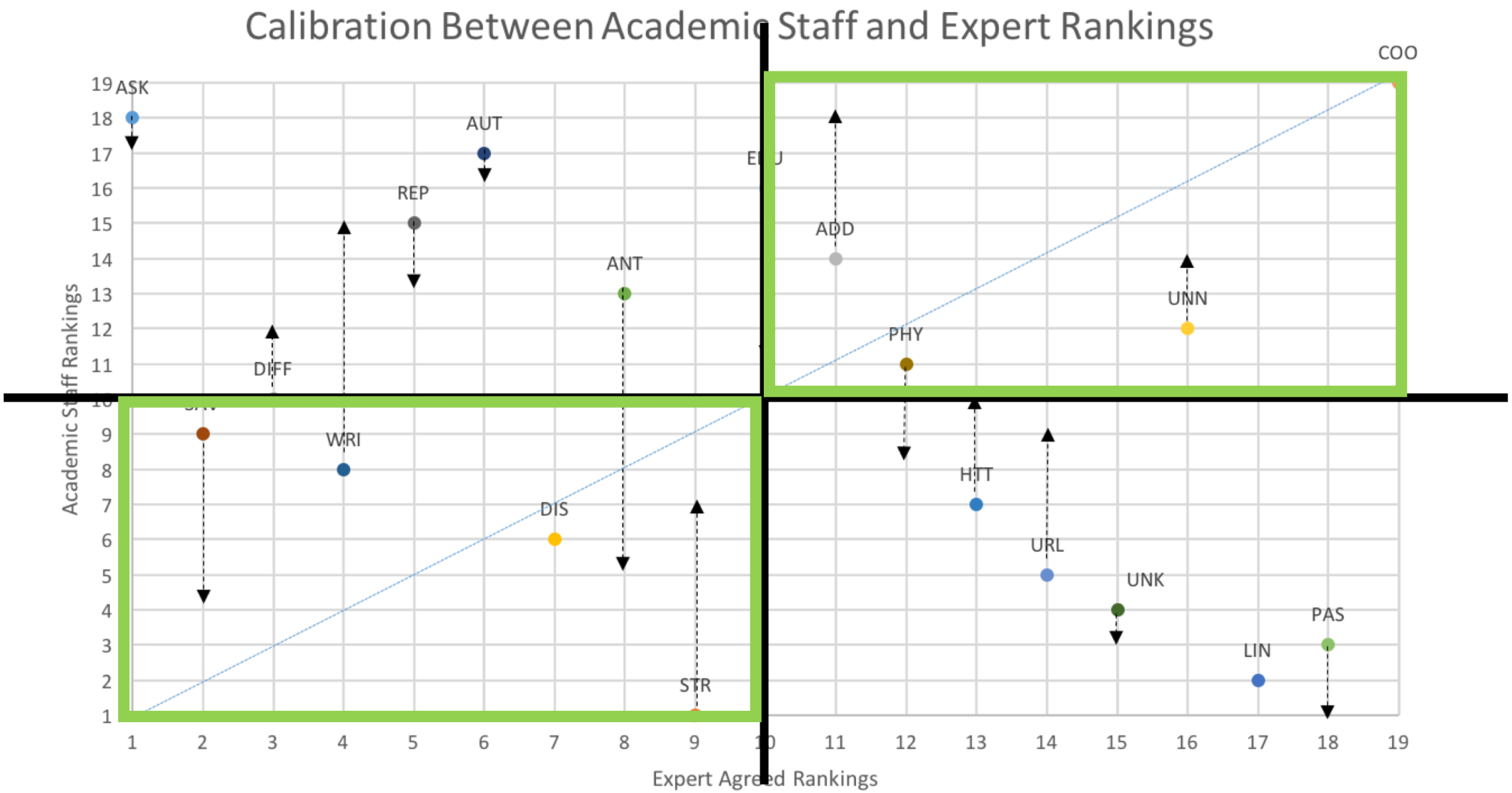
Northumbria University NEWCASTLE

Example Output: Discrepancies



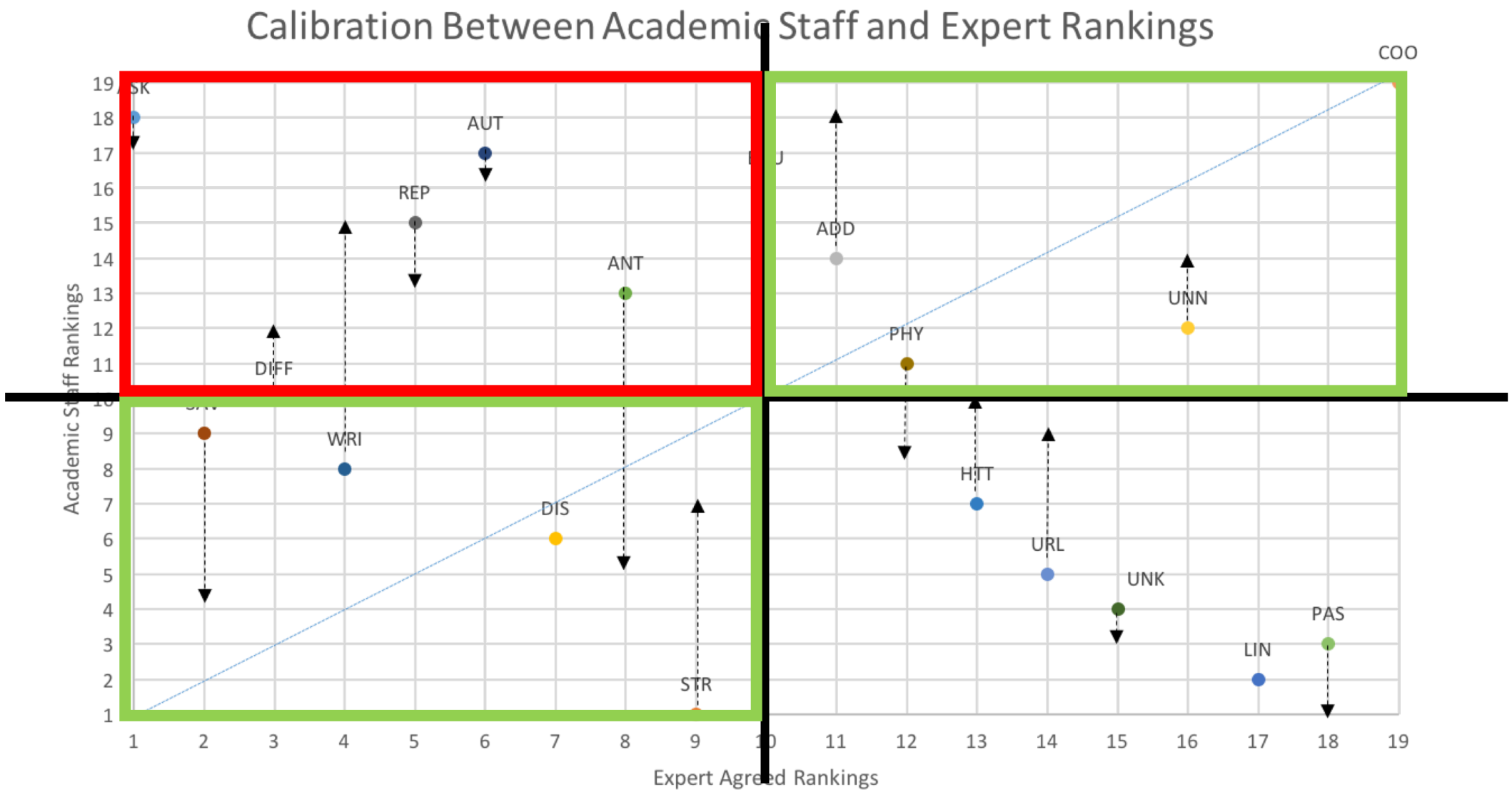
Northumbria University NEWCASTLE

Example Output: Discrepancies



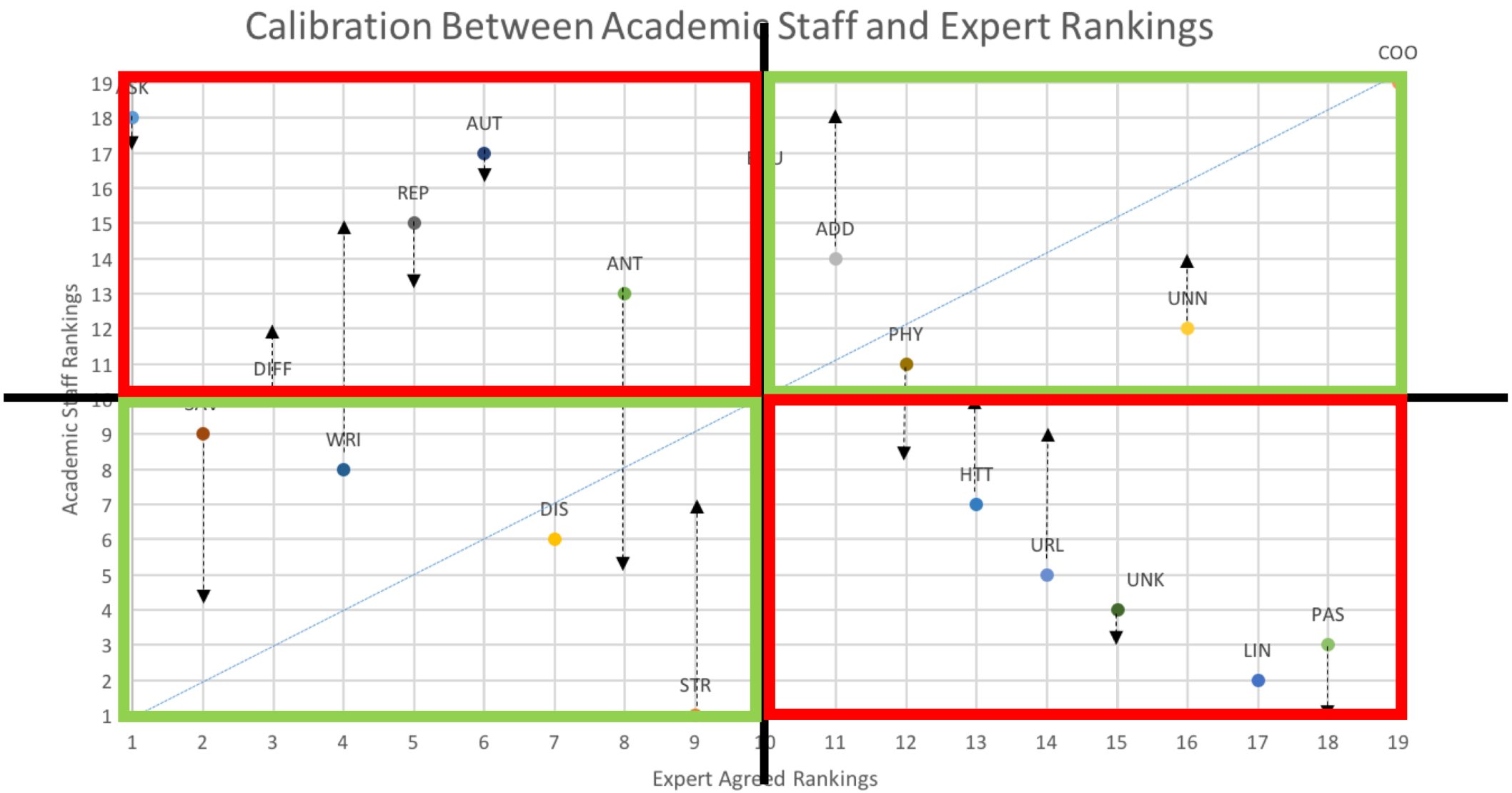
Northumbria University NEWCASTLE

Example Output: Discrepancies



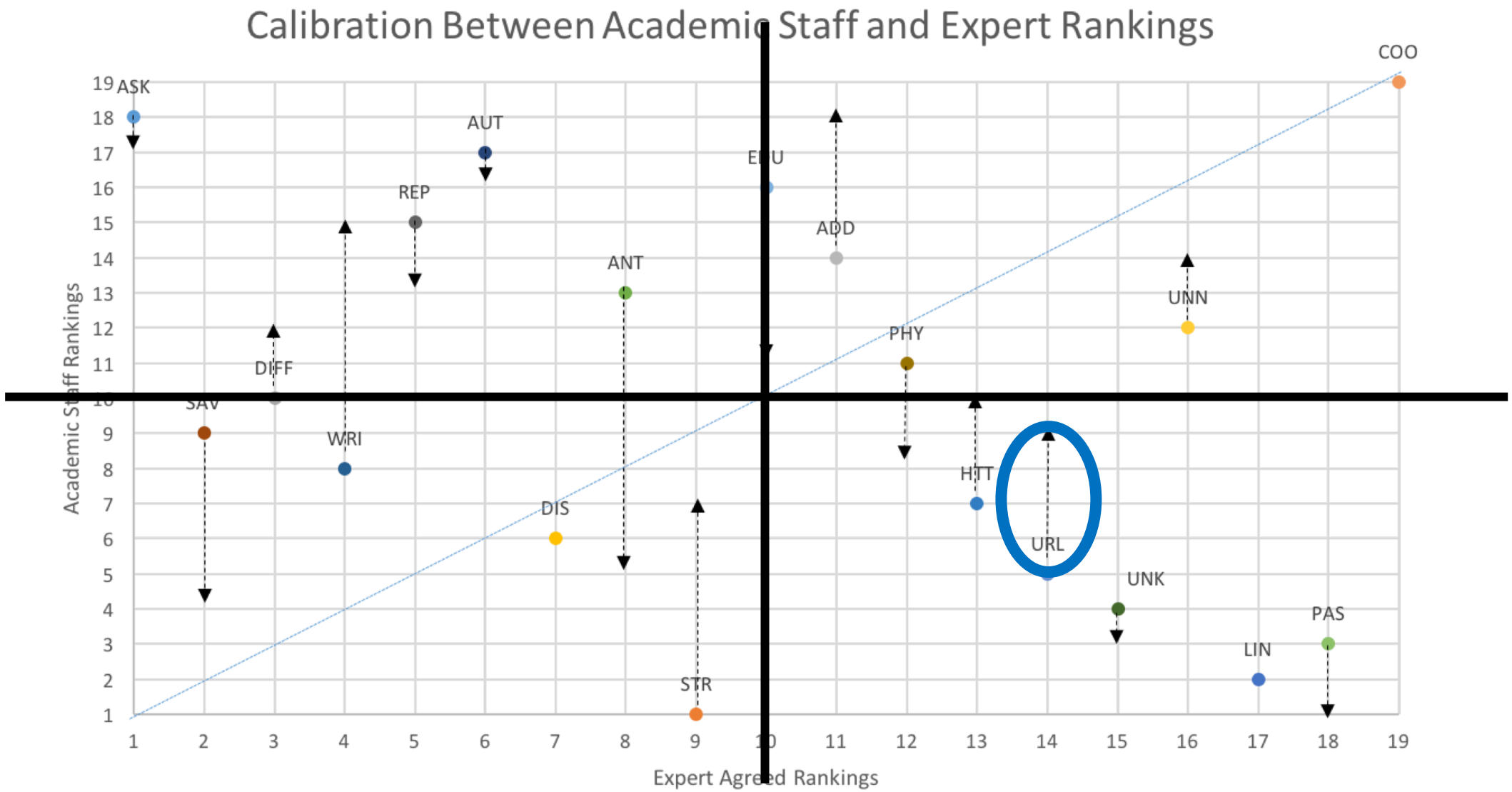
Northumbria University NEWCASTLE

Example Output: Discrepancies



Northumbria University NEWCASTLE

Example Output: Discrepancies



Northumbria University NEWCASTLE

Example Output: Flawed Mental Models

Academic Group 2 (Female 1): "But if you opened it, I wouldn't anyway, but open an attachment from someone I didn't know – I would just delete it – but if I did open it I would assume that unless I clicked on a link within that attachment then the attachment couldn't, unless, you know like a Word attachment, if they sent me some kind of attachment that could be actually downloading a virus."

Northumbria University NEWCASTLE

Feedback from Experts

CISO: “I have, based on years of experience, developed a prejudice towards certain desired behaviours that I now think, based on this, perhaps I’ve allowed that prejudice to drive my own personal baseline. And I think this tool helps break that and forces me to re-evaluate my concept of desired behaviours.”

Northumbria University NEWCASTLE

Strengths and Weaknesses

- Ranking task, so less social desirability
- Specific to each organisation
- Provides cybersecurity insights for both employees and experts

- Overall duration (for deployment 2): 5 hours and 15 minutes
- Needs evaluation in different industries

Northumbria University NEWCASTLE

Summary: The Cybersurvival Task

- Task where employees have to rank a list of (organisation-specific) behaviours in order of importance for staying safe online
- Allows for identification of disagreements between organisational security experts and employees
  - Identify misconceptions and shadow behaviours
  - Experts can tailor training or awareness programme to these behaviours
  - Experts can rethink their policies

You could ask me about:

- What differences did you observe across job roles?
- You mentioned interesting heated discussions. What were they fighting about?
- What else were the experts surprised by?
- What are your pearls of wisdom if I want to run this task?

e: james.nicholson@northumbria.ac.uk

t: @jjnicholson

w: www.jjnc.xyz

Northumbria University NEWCASTLE

EPSRC Engineering and Physical Sciences Research Council