Cyber Security Culture...a different view

Sociotechnical Security Group
NCSC & The Sociotechnical Security Group (StSG)

NCSC: “Make the UK the safest place to live, work and do business online.”

Centred on: risk, people and security and engineering processes and assurance

Looking at the intersections of these topics and look broadly at the research.

My role:

Researching people and security for over 7yrs

Develop a deeper understanding of how to engage and understand the drivers of people in cyber security
“I want to make sure that security is working in my business. How can I get people to pay attention?”
“People are the weakest link in organisations, why don’t they just pick better passwords”

“why don’t people just do what they are told, its simple!”

“People are lazy”
Engagement is often done through training.
This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk
We use ingenuity to succeed in our jobs

Navigate difficult policies, processes or unusable IT.

How do people get their jobs done?

Is security really working the way you expected?

People bring a lot of knowledge of how things actually work in the organisation, use it.

Understand how their creativity manifests itself in everyday work.
Engagement & collaboration needs the right culture:

The organisation visibly learns from mistakes and problems by changing systems reducing the opportunity for the same events to reoccur.

A structure for reporting events should be in place.

Staff must trust that they will not be automatically blamed for reporting errors or problematic situations.
Mini Revelations

Don’t call people users

Stories are very powerful: but must be relatable

Must look at what goes right, instead of focusing on what goes wrong

People liked to be involved and asked their opinion.

Creating dialogue will go along way to break down barriers.
People are part of the solution not the problem