Interview transcripts are not made available here as they may contain sensitive information or information that might make it possible to identify participants and their organisations.

Research Notes

These notes are collated from themes found across notes from each interview.

- De-risking innovation through initiatives.
  - Helping with commercialisation and lack of investment.
- Status of cybersecurity relatively low.
- Contrast in quantity of guidance for organisational security verses for products.
- Standards not consistently implemented.
- Guidance is confusing.
  - Too generalised.
  - Heterogenous.
  - Difficult to know what to use.
  - Governance needed.
  - Different jurisdictions for guidance.
- Some sectors are more security cautious than others.
  - Different views on whether organisations see themselves as part of connected places.
- Local authorities need more specific guidance.
  - Potentially procurement guides.
- Demand side lacking in resources to achieve best practice.
  - In theory, the rewarding of contracts should incentivise best practice.
- Differing security maturity levels between sectors.
- Initiatives for information sharing exist but there are barriers to this (market driven) that could be improved.
- Incentives need to be considered alongside capability.
- The need to make sure the right cybersecurity skills are being fostered.
  - Importance of training.
- Responsibility diffused throughout the supply chain.
  - Impulses to outsource risk and responsibility.
- The need to establish principles to make sure organisations are working towards the same thing.
- Need to raise cybersecurity awareness.
  - Addressed by some innovation/accelerator programmes.
  - Status of cybersecurity is improving – impact of media.
  - Poor understanding of risk in many organisations.
- Mixed or low engagement with guidance among SMEs.
  - Cybersecurity of lower priority and addressed later down the line.
  - Concern that SMEs may not have the resources to implement best practice.
- Need to reframe cybersecurity as a way to improve business.
- Different definitions of cybersecurity.
  - Important for incentives.
- Pattern of incentives according to supplier size.

- Need for citizen-centric approaches to data.
    - E.g., citizen ownership of data.
    - User-led innovation.
- Need to build trust with customers – who are the customers and the users?
- Considerations of responsibility towards citizens of connected places.
- Concern around GDPR and more responsibility taken for data protection.
- Metaphors for cybersecurity – unexciting, difficult to justify investment.
- Emphasis on innovation and the need not to stifle it with requirements.
- Not enough market incentives for cybersecurity best practice.
- There is a need still to help people know what "good" looks like.
- Some indication of the need for regulation.
- Customer awareness is not high yet and could potentially incentivise best practice.

<u>Notes from initial of analysis of interview results</u>

1. Best practice
    a. Where people look
    b. Is guidance effective?
        i. Guidance is on a principles level but lacking specific actions
        ii. Secure tech vs secure business
        iii. A confusing landscape
    c. Information sharing is successful in building connections across the ecosystem
2. Achievability
    a. Resources
        i. Funding is used to mitigate risk
        ii. Skills
        iii. Opposing views that it is achievable
    b. Procurement structure in connected places
        i. Difficult to specify requirements
        ii. Ways to ascertain good practice
3. How well does it foster best cybersecurity practice?
    a. Status of cybersecurity
        i. Fear of stifling innovation
    b. Incentives
        i. Citizens and trust
        ii. Cybersecurity as a pain
        iii. Social responsibility
    c. Problems stopping cybersecurity being fostered
        i. Governance
        ii. Disincentives naturally come up in discussion of incentives
            1. People naturally go on to talk about what is failing
            2. Awareness problem