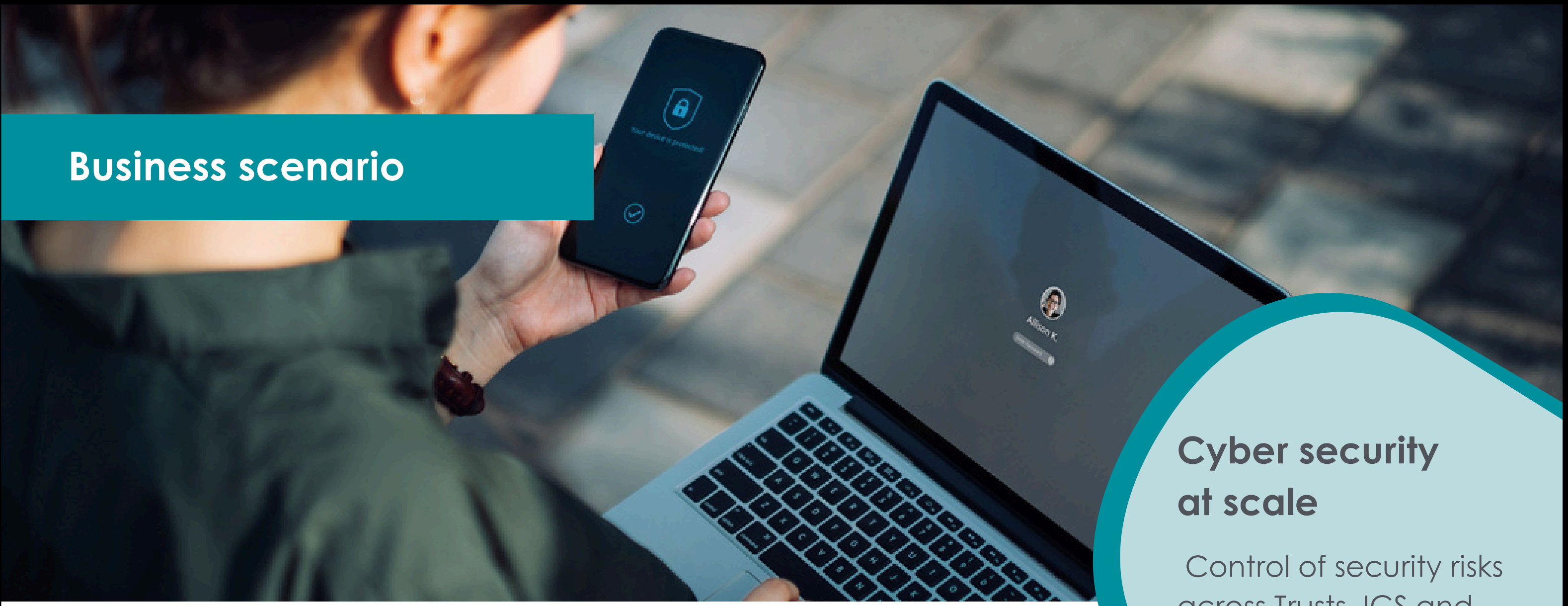

Business scenario

Cyber security at scale

Control of security risks across Trusts, ICS and regions

Securing clinical services at scale through improved cyber security

Within NHS Integrated Care Boards (ICB), each individual Trust typically has its own dedicated Digital, Data and Technology (DDaT) services.

DDaT services can often be seen as a blocker by Healthcare professionals, where security policies and practices can limit or even prevent clinical innovation or restrict access to key systems or sources of data without lengthy security reviews.

Improvement in cyber security standards to develop trust networks will better support clinical need, guarantee security, and provide greater opportunities for clinical collaboration, ensuring that DDaT can be viewed as an enabler for patient care, rather than a blocker.

Challenges

Difficulties in **maintaining security on mobile workforce devices** that can move between sites and span a number of different types, models and ages, potentially **leaving clinical services vulnerable to cyber-attack**.

Significant **operational overhead** in supporting the security of technical and digital services across a **range of internal, shared and cloud-based platforms**.

Monitoring multiple **cyber security risks in IT and digital services** as well as the **connected technologies** that support clinical service delivery requires a wide understanding of how to defend against cyber risks.

Patient data contains a range of **protected characteristics**, and all data can be considered **highly sensitive**, so protecting data shared across **many clinical services** is a major healthcare challenge.

Solution approach

Agree a **minimum standard** for all end user devices, and replace **older technology**, so that all devices can be **kept up to date** to offer the best level of protection.

Cooperate on key **shared cyber security services** such as a Secure Operations Centre (SOC) to improve the **operational effectiveness**, and better manage the **cost of these specialist services**.

Agree **standards for data classification** of patient data across all technical and digital services. Agree **clear data classification** rules that will govern the use of and **protect data from unlawful access**.

Include **security standards as part of the technical architecture** that can be shared with all technology providers, including clinical technologies.

Benefits

Security is a vital component to any modern digital healthcare system, and as such security services must engender trust in technology:

- Standards for security provide **greater flexibility** for clinical staff to share information and **collaborate on clinical decision making**.
- Centralised cyber services allow for multiple organisations to react to threats more effectively, helping to maintain a secure working environment.
- Patients are more willing to **utilise digital services**, and share data electronically if they know their **data will be secure**.
- **Reduced risk to cyber security attacks** leading to a loss in services, allowing clinical staff to focus on **patient care**.

masonadvisory