24/03/2023

Cyber Security Strategy for Health and Social Care

Earlier this week the new long-term strategy for creating a cyber resilient Health and Social Care system in England was launched. The Cyber Security Strategy for Health and Social Care provides a high-level view of the whole system's needs up to 2030, breaking down the individual challenges and action for the different sectors. The strategy uses 'defining roles' to clarify how the commitments will look for each part of the system, with the role of National-first being a source of guidance and an enabler for shared learning rather than being directive. The roles are as follows:

- National and regional cyber security teams
- Integrated care systems (ICSs)
- Health and social care leaders – Including Senior Leadership and Board-level.
- Cyber workforce – key roles in cyber security such as Chief Information Security Officers.
- Third party suppliers - any organisation providing goods or services to the health and care sector.
- All employees – anyone working in Health and Adult Social Care, delivering care and support.

The strategy's main aim is to 'bake in' cyber security into the sector's processes to ensure the commitments and trust required to making Data Saves Lives and the Digital Health and Care Plan a reality are not undermined by vulnerabilities, such as the recent Advanced ransomware attack (used as a case example to forecast how future threats will be enacted). Although the strategy makes mention of Data Saves Lives, it does not detail anything about data or the connections required for sharing it across Health and Social Care, this is not within its scope, this is currently underway with SOCITIM Advisory's leading the commissioned work building a minimum operational dataset and terminology .

The strategy vision has its sights set for 2030 where we will see:

- The risk to organisations of a cyber attack is reduced.
- Patient and service user data is protected.
- Organisations are able to respond and recover quickly to any cyber attack.
- Patient trust in the sector's digital systems is increased, and technological innovations can be applied with confidence.

Its commitments are viewed through 5 pillars:

1. **Focus on the greatest risks and harms** - to understand the most critical parts of the health and care sector whose disruption would cause the greatest harm and ensure they are proportionately protected.

This includes:

- Developing a common language for measuring and recording risk at a national level and building a system-wide threat picture. This will make threat information sharing more efficient so that the whole system can respond.
- This will support organisations to regularly review their systems and security, developing plans that mitigate risks.

2. **Defend as one -** to ensure the health and care system understands its interdependencies and takes advantage of its scale to present a centralised, united front. This means ensuring the sector benefits from national resources and expertise, employs collective leverage capabilities, and adheres to clear and consistent standards. This includes:

- National Teams being less directive but instead enable an environment of sharing learning and providing a clear picture of where standards and requirements need to be adhered to. The strategy acknowledges that organisations should remain autonomous and able to adapt their approach to cyber security to meet their needs.
- The strategy defines the joining up of resources and shared learning across Health and Social Care as a partnership. This point, along with the one above, acknowledges Social Care as a sector independent of health, which we want to see translated in the forthcoming implementation plan.
- National shared learning and initiatives will support leaders to decide where to invest as well as how to initiate security monitoring across the whole organisation.

3. **People and culture -** to build a health and care system in which leaders, cyber professionals and generalist staff understand and are skilled to undertake their role in relation to cyber security. Growing a profession of cyber experts in health and care will be key to recruiting and retaining the expertise needed to achieve this. This includes:

- A national approach to joining up all systems in a collaboration of Health, Government, Social Care, Commercial Third Parties and Academia to ensure alignment and sharing of learning.
- A national commitment to ensuring cyber basics training and guidance is available. This will support all care and support staff to be more knowledgeable on best practice and understand the importance of this in their work.
- Embedding a 'no blame' culture to cyber, the NHS's Just Culture is used as the example of good practice. This promotes a culture of openness and honesty, which has parallels with embedding the Duty of candour.
- Leaders should take ownership of cyber security decisions as well as growing cyber roles in their organisation. This will be a difficult commitment to achieve without funding and we want to see this addressed in the workforce plan mentioned in the bullet point below.
- The need for more Cyber Roles. There is an intention to bring forward a plan to develop health and care's own cyber security workforce by 2024. This is separate to the Digital Workforce Development Plan due in Spring this year.

4. **Build secure for the future -** to embed security into the architecture of emerging health and care governance and technology from the very beginning so that cyber security is increasingly applied by default. This includes:

- Working with commercial suppliers at a national level to minimise risk in the supply chain. A good example of how this could be achieved is the Assured Supplier List for Digital Social Care Records.
- Building the Cyber Assessment Framework (CAF) into the Data and Security Protection Toolkit (DSPT). The aim is to map the DSPT directly against the CAF by 2024, aligning the DSPT to be CAF-based by 2025. We would like assurance as to how achievable the CAF is for providers and we will work with colleagues from Better Security, Better Care and Digital Social Care to ensure the voice of providers informs this.

- Leaders and cyber professionals are able to operationalise national guidance and standards, maintaining a list of critical suppliers and their cyber status alongside building in good cyber practice with teams when adopting new technology.

5. **Exemplary response and recovery -** to support every organisation in health and care to be able to minimise the impact and recovery time of a cyber breach when it occurs – both directly and through promoting best practice and building capability. This pillar's focus is on the development and dry run of cyber response plans, ensuring that the processes are in place to enable the plan to be enacted adequately.

In working towards this strategy's vision, the national cyber security team's aims are as follows:

- continue to enhance the NHS England CSOC and develop a framework to support local security operations centres - **by 2024**
- update the DSPT to reflect the CAF, empowering organisations to own their cyber risk - **by 2025**
- provide funding for local cyber resource with national training support - by 2025
- publish a comprehensive and data-led landscape review on the status of cyber security in adult social care, spending at least £15 million over the next 2 years in response to that review - **by 2025**
- develop a product to map our most critical suppliers, engaging with them through dedicated channels and supply chain summit - **by 2024**
- publish an implementation plan setting out planned activity for the next 2 to 3 years to support meeting the aims and goals of this strategy - **by summer 2023**

You can take proactive steps as a provider now, using these free resources:

- If you are a CQC Registered Provider, make sure your Data Security and Protection Toolkit is up-to-date:
  - Support for publishing for the first time.
  - Support for republishing.
- Join Towergate's Cyber Security and the Continuing Changing Environment Webinar on 18th April 10:00-12:00.
- Take advantage of the free Immersive Labs licenses for ASC.
- Share these Top Tips for strengthening your cyber security.