A RICOH Company

Cyber Security Strategy

East Suffolk & North Essex NHS Foundation Trust (ESNEFT)

Case Study

About ESNEFT

East Suffolk and North Essex NHS Foundation Trust (ESNEFT) provide hospital and community health care services for Colchester, Ipswich, North East Essex, and local areas. Formed on 1 July 2018, ESNEFT is the largest NHS organisation in Suffolk & North East Essex Integrated Care System. They also provide community services in Suffolk and both Colchester and Ipswich hospitals have major accident and emergency (A&E) departments.

Like all NHS Trusts they are an operator of essential services to the communities they serve. They must protect those services from disruption and keep patients, carers and staff safe, their data confidential, accurate and available for use in clinical and care decision making.

Challenges

The Digital, Data & Technology team has 300 staff who support 12,000 colleagues and devices. The team had recently grown through a merger and had adapted to support new ways of working during the Covid Pandemic. Cyber Security was recognised as a growing risk to their services and, though great effort was put into compliance with regulatory requirements, principally the Data Security & Protection Toolkit (DSPT), the Trust had struggled to reach compliance goals regularly enough.

They recognised the need to take a more strategic approach to Cyber Security Resilience so approached MTI, who were working with Suffolk and North East Essex Integrated Case System (SNEEICS) on cyber risk reduction in the region, to help shape a Cyber Resilience Strategy and Security Target Operating Model.

Why MTI

NHS 75
East Suffolk and North Essex
NHS Foundation Trust

Detailed understanding and experience delivering services to NHS organisations

Operational understanding of the Cyber Security Strategy for Health & Adult Social Care

30-year experience in Cyber Security industry with NCSC CHECK status for penetration testing

Understanding, flexibility and patience to work with the Trust at our pace

Previous work with the Integrated Care System to improve cyber resilience

Depth of experience in Cyber Security across people, process and technology

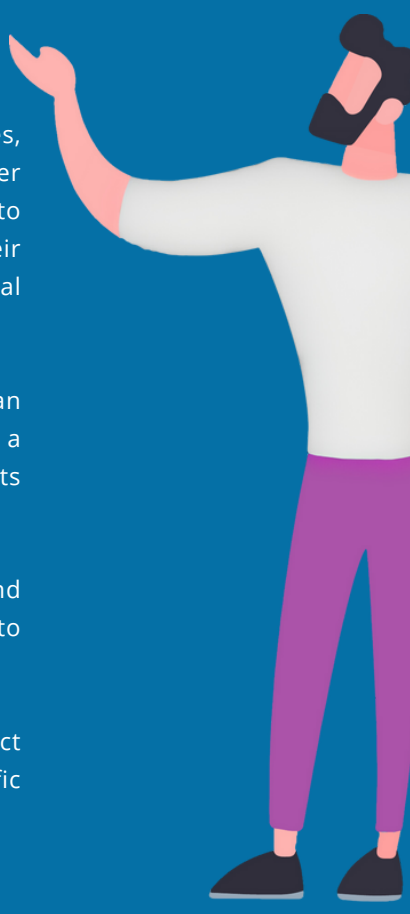
> **MTI has played a crucial role in shaping our Cyber Security Strategy, previously we felt we were being reactive. With the volume of work coming in and the ever-evolving threat landscape, we recognised the urgent need for a more structured and comprehensive strategy. With their expertise and guidance, the MTI team brought a panoramic view of the NHS, enabling us to grasp the bigger picture. They not only provided valuable insights into the national agenda but also ensured our alignment with it—a luxury we simply couldn't afford to pursue independently. Thus, MTI stepped in, and we are delighted with the results of our collaboration on the cyber strategy. The feedback from everyone has been overwhelmingly positive, impressed by the accomplishments we have achieved together.**

Mark Caines
Associate Director of
ICT, Digital & Logistics

Results & Benefits

ESNEFT have rebalanced their efforts toward assessing and reducing Risks. They have a Cyber Security Strategy that will see them "Get Ahead & Stay Ahead" of evolving threats and compliance objectives over a 3-year period. The Strategy and Operating Plan will enable resilience and security by design with compliance achieved by default.

- Proactive Cyber Security Strategy:
  - The Trust's cyber resilience strategy aligned with digital transformation initiatives, national strategies and evolving compliance requirements (NIS / NCSC Cyber Assessment Framework). This ensures a robust and proactive approach to safeguarding sensitive data and systems and helps all staff to recognise their responsibility to keep ESNEFT secure and patients safe in an increasingly digital world.
- Future Focused Mentality:
  - Get Ahead, Stay Ahead and Innovate – a long term, future proof strategy and plan with realistic milestones to achieve over the next 3 years and early planning for a further 3-year period. This empowers the Trust to stay ahead of evolving threats and compliance requirements.
- Enabling Innovative Projects:
  - By providing dedicated time and resources, MTI enabled ESNEFT personnel to spend the time needed to think and plan. They embedded cyber resilience into organisational transformation and new Electronic Patient Record programme.
- Leveraging NHS connections & knowledge:
  - The NHS expertise MTI holds enabled them to share insights, and connect organisational with national and regional strategies. ESNEFT have a strategy specific to their own need and aligned with the rest of the NHS system to defend as one.



Solution

MTI adopt a unique approach to developing a cyber resilience strategy for our customers. We recognise that everyone in an organisation must buy into and adopt a strategy for it to succeed. It's unlikely strategic initiatives will achieve their objectives if they're driven from the board without business and operations teams being fully invested. Conversely any strategic initiative driven from the ground up will fail without the full support of the board, a solid plan and appropriate budget.

The MTI approach combines "top down" and "ground up" to define both organisational and granular objectives with a structured, prioritised plan to achieve them.

With ESNEFT, we began with a review of existing evidence, in this case DSPT Audit Report, Security Policies, Penetration Testing and Vulnerability Register. A summary report was produced that groups risks and issues into categories and suggests a priority for remediation. The report was used to inform the overall strategy and stakeholder interviews. Workshops were conducted with people from all levels and across the organisation (Digital, Data & Technology, Clinical and Nursing, Risk, People & Communication, Finance etc).

A **Cyber Resilience Strategy** is built to reflect the specific landscape of the organisation and align with its other strategies and programmes. This is delivered in the form of a presentation and written document for the organisation to put into a format of their choice and approved by board. Finally, we mapped the strategic and granular objectives in a Traceability Matrix that captures who is Responsible, Accountable, Consulted and Informed (RACI) for each objective with a target timeline. If budget is not in place for an objective our team can support with building a business case.

About MTI

MTI Technology is a highly-experienced, multi-award-winning technology services and solutions provider, with over 3 decades of experience in data centre, cyber security and managed services. We operate across Europe, with offices in the UK, France and Germany. In 2020, MTI was acquired by Ricoh as part of their transformation into a global digital services company. MTI is a key constituent in Ricoh's IT services growth and investment strategy. MTI's mission is to build a secure digital future for our customers, and its vision is to be the leading hybrid infrastructure and cyber security services and solutions provider in the markets we serve.

Deliverables

- Granular report – categorising common risk areas and setting priority.
- Cyber Resilience Strategy – detailing organisational objectives.
- Traceability Matrix – RACI for each objective.

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200

A RICOH Company