CASE STUDY

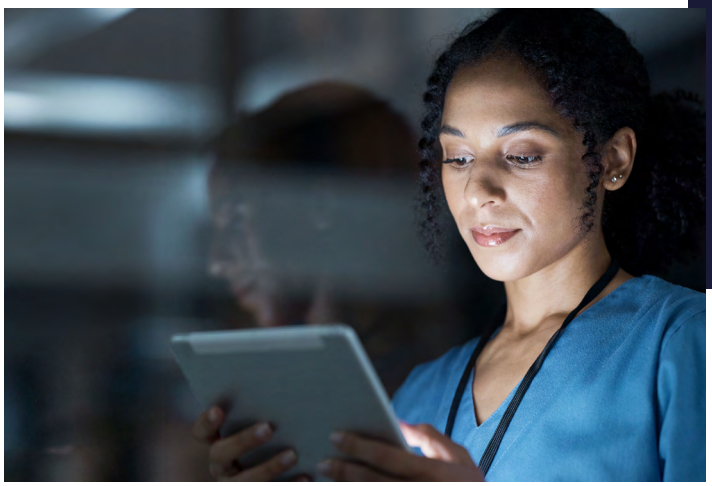
Enhancing Cyber Security through Supply Chain Assurance and Risk Framework

NHS
Hertfordshire Partnership University
NHS Foundation Trust

Overview

Hertfordshire Partnership University NHS Foundation Trust provides health and social care for over 400,000 people, helping those suffering with mental and physical ill health, and learning disabilities across Hertfordshire, Buckinghamshire, Norfolk and North Essex. Employing around 4,000 people, these services are delivered both within the community and in inpatient settings.

The Trust relies on the outsourcing of various services to ensure that it continues to run within its financial constraints. The supply chain is a particular attack vector that the NHS needs to increasingly assure against as cyber threat actors look to incapacitate vital services or compromise confidential and critical patient data.



The Challenge

The organisation faced several formidable challenges that necessitated a comprehensive and robust approach to secure their supply chain.

With an extensive and complex network of suppliers, service providers, and partners, the Trust needed a 360-degree view of their supply chain and the levels of risk they were tolerating, enabling them to plan for improvements. Moreover, they needed a way to better assess prospective suppliers on their cyber security practices and generate a risk score so that they could more confidently and independently risk assess new suppliers.

Hertfordshire Partnership University NHS Foundation Trust chose i3Secure to carry out their supply chain assurance and risk framework because they recognised that i3Secure's specialist consultants have extensive experience working within the NHS and a deep understanding of the unique cyber security challenges faced by healthcare organisations, including their regulatory compliance obligations such as DSPT.

Furthermore, i3Secure's reputation for flexibility and reliability as a consultancy partner played a crucial role in the decision-making process. Their ability to adapt to the Trust's schedule and work harmoniously with stakeholders demonstrated a commitment to ensuring a seamless and efficient engagement.

Our Solution

i3Secure's consultant initiated the process by thoroughly researching each supplier that the Trust had existing contracts with, validating their security certificates, such as ISO 27001 and Cyber Essentials. These credentials were meticulously catalogued and presented to the Trust, along with renewal dates for each certificate, empowering the organisation to proactively monitor their suppliers' certificates and conduct future due diligence.

Subsequently, an in-depth analysis of the terms and conditions for frameworks utilised by the Trust was conducted, highlighting the obligations to which suppliers were subject to, before being accepted into those frameworks. An extensive examination of contracts was undertaken, with the objective of extracting detailed security requirements for each supplier. These findings were organised into a comprehensive matrix, allowing the Trust to gain a holistic perspective and verify that current requirements were appropriately aligned with each supplier.

To provide a more permanent solution for future supplier risk assessments, i3Secure's consultants developed a Cybersecurity Maturity Assessment for the Trust. This assessment adopted a similar format to the Cybersecurity Maturity Model Certification (CMMC) developed by the US Department of Defence and incorporated a scoring mechanism, which also considered applicability. This approach ensured that the Trust could accurately assess and gauge prospective suppliers' cyber security maturity, facilitating well-informed decision-making and enhanced supply chain assurance.

The Result

As a result of the engagement, the NHS Trust achieved comprehensive oversight over its supply chain risk landscape, enabling them to confidently engage with new and existing suppliers.

Continuous monitoring was established to help manage third-party risk, giving them an overview of their entire vendor ecosystem and allowing them to independently assess their cyber security maturity using the Cybersecurity Maturity Assessment.

Transparent communication channels were set up between the Trust and suppliers, enabling prompt response to cyber security concerns and provide more proactive incident management.

i3Secure's consultants advised the Trust on pre-procurement standards so that they could work to a minimum threshold of security that vendors must meet before moving forward, neutralising the risk to their systems and networks.

In summary, Hertfordshire Partnership University NHS Foundation Trust was able to help reduce the risk of cyber-attacks resulting from vulnerabilities within the supply chain and minimise the threat landscape across the Trust, avoiding devastating, expensive and long-term ramifications for the organisation, their supply chains and their patients.