CASE STUDY

Empowering Cyber Resilience in the NHSx COVID Pass and Letter Service

Overview

Launched in 2021, the NHSx COVID Pass and Letter Service was a critical initiative by the NHS to provide digital COVID-19 vaccination certificates and official vaccination letters to individuals. The service played a vital role in enabling safe travel and access to various venues during the COVID-19 pandemic.

NHSx required a dedicated Cyber Security Risk Manager for their COVID-19 Pass and Letter Service. This would bring specialised expertise in identifying, assessing, and mitigating vulnerabilities that could compromise the service's security and integrity.

The role demanded an experienced consultant to assume accountability for the Cyber Security Risk Register and associated tasks. These included identifying digital assets, reviewing existing security measures, and either continuing what was working or mitigating security risks that may pose threats.

i3Secure was appointed to support the Service due to our specialised expertise in healthcare cyber resilience, having worked with numerous NHS Trusts providing cyber security and information assurance consultancy. Our understanding of and flexible approach towards challenges faced by the NHS were key factors for the client in making this decision.

The Challenge

Faced with strict time constraints, NHSx sought an accomplished consultant to oversee the efficient administration of their Cyber Risk Register. The consultant had to:

- Conduct risk assessments to identify potential vulnerabilities in the Trust's IT systems, networks, and applications that could lead to cyber threats, data breaches, or operational disruption.
- Understand current and emerging cyber risks such as ransomware, phishing, or data breaches, and how they could impact healthcare operations.
- Design and implement strategies to mitigate or manage identified risks. This involved introducing new technologies, processes, or policies.

This included a continuous cycle of identifying, analysing, evaluating, and mitigating NHSx's cyber security risks.

The client required a consultant with significant risk management experience who could assume a multifaceted role. Their role would range from urgent threat prioritisation to strategic vulnerability management, and from threat modelling to fraud risk guidance. Rigorously executing these responsibilities, our consultant played a pivotal role in securing the Service and strengthening cyber resilience amidst evolving threats.

© 2023 i3Secure Ltd

Our Solution

Thanks to i3Secure's flexible engagement approach, we were able to promptly deploy a seasoned Cyber Risk professional for a four-month tenure, meeting the immediate demands of the role.

Our appointed Cyber Risk Manager conducted an exhaustive assessment of the service's digital infrastructure, data handling procedures, and third-party integrations. This identified potential vulnerabilities and helped us formulate a robust risk mitigation strategy to address these weaknesses.

We implemented a comprehensive cyber security framework designed specifically for the healthcare sector, aligned with industry best practices and regulatory standards. This included:

- Data encryption to protect sensitive data.
- Access controls to ensure only authorised personnel could access critical systems.
- Intrusion detection mechanisms to quickly identify potential breaches.
- Incident response plans to ensure quick and effective responses to any security breaches.

We carried out regular penetration testing, identifying and addressing critical vulnerabilities before they could be exploited. For example, we uncovered and resolved 12 high-risk vulnerabilities, strengthening the system's overall cyber resilience.

Our Cyber Risk Manager orchestrated specialised training sessions for NHSx team members, improving their awareness of cyber threats, social engineering tactics, and optimal security practices. This proactive approach helped staff recognise and avoid potential risks, fostering a more secure operating environment.

i3Secure played a pivotal role in assisting NHSx in crafting a comprehensive incident response plan. This detailed the exact steps for communication, containment, eradication of threats, and post-incident recovery. By preparing NHSx for potential security breaches, we ensured the team would respond swiftly and effectively.

The Result

i3Secure's engagement led to substantially improved cyber resilience across multiple facets of the COVID Pass and Letter Service's cybersecurity infrastructure:

Reduced Vulnerabilities
Through penetration testing and remediation efforts, we significantly reduced the potential for exploitation.

Enhanced Threat Detection
Integrating advanced intrusion detection mechanisms, we improved real-time threat detection significant, allowing for quicker responses to potential breaches.

Strengthened Incident Response
The newly implemented incident response plan was tested and refined, ensuring a faster and more effective reaction time to security events.

Compliance and Confidence
NHSx was able to meet regulatory compliance requirements more efficiently, with the assurance that the service was operating under robust security measures. This helped to bolster user confidence in the system, particularly important as the service expanded.

By end of contract, i3Secure successfully handed over the Cyber Risk Register to the Programme Management Office RAID Lead, ensuring a seamless transition of responsibilities and continued risk management.

© 2023 i3Secure Ltd