The target operating model for cyber security in healthcare

The target operating model for cybersecurity in the NHS should be designed to effectively manage and mitigate cyber risks, protect sensitive patient data, and ensure the continuity of healthcare services. While the specific details of the target operating model may vary based on the unique needs and circumstances of each NHS organisation, here are some key elements that should be considered:

Centralised governance and leadership

Establishing a centralised governance structure with clear accountability and leadership is essential. This include designating a Chief Information Security Officer (CISO) or an equivalent role responsible for overseeing the cybersecurity strategy, policies, and operations across the organisation. Centralised governance ensures consistent implementation of cybersecurity measures and enables effective decision-making.

Risk management framework

Implementing a robust risk management framework is critical to identify, assess, and prioritise cyber risks. This framework should include processes for regularly assessing the organisation's threat landscape, evaluating vulnerabilities, and determining appropriate risk mitigation strategies. It should also incorporate incident response planning to ensure a timely and coordinated response to cyber incidents.

Security operations center (SOC)

Establishing a Security Operations Center (SOC) or a similar function can provide round-the-clock monitoring, detection, and response capabilities. The SOC should be equipped with advanced threat detection tools, security information and event management (SIEM) systems, and skilled personnel to monitor network traffic, analyse security events, and promptly respond to potential threats or incidents.

Collaboration and information sharing

Promoting collaboration and information sharing within the NHS and with external stakeholders is crucial for enhancing cybersecurity. Encouraging partnerships with other NHS organisations, sharing best practices, and leveraging threat intelligence sources can help identify emerging threats and vulnerabilities. Collaborations with external cybersecurity organisations, industry experts, and government agencies can provide additional expertise and support.

Employee training and awareness

Investing in comprehensive cybersecurity training and awareness programs for all staff members is vital. This includes educating employees about common cyber threats, phishing scams, password hygiene, and safe online practices. Training should be regularly updated to address emerging threats and promote a culture of cybersecurity awareness across the organisation.

Third-party risk management

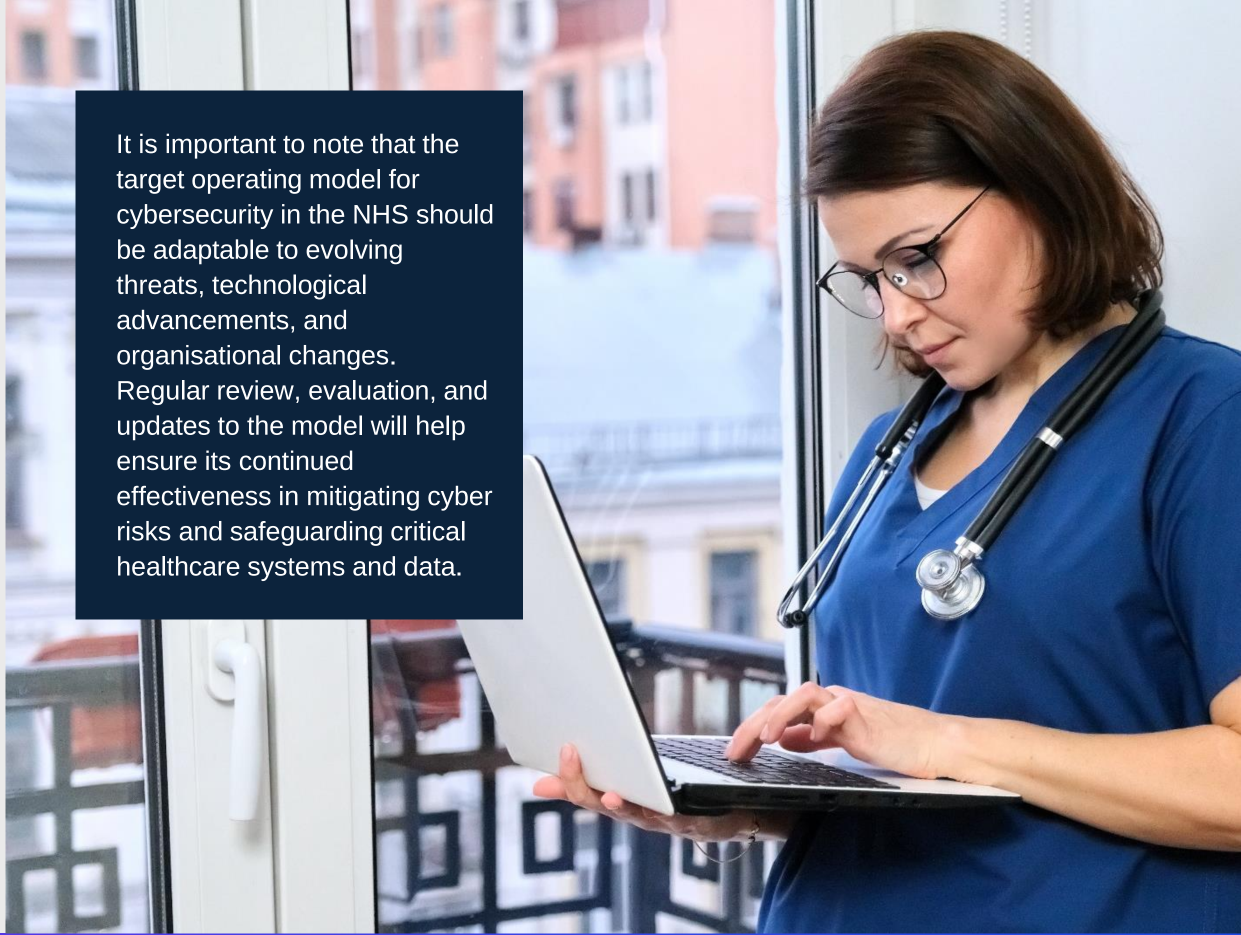
Given the interconnected nature of healthcare systems, it is essential to effectively manage third-party risks. NHS organisations should implement processes for assessing the cybersecurity posture of third-party vendors, contractors, and service providers. Contracts and agreements should include clear cybersecurity requirements and regular audits to ensure compliance.

Continuous monitoring and assurance

Implementing continuous monitoring and assurance mechanisms is crucial to proactively identify vulnerabilities and address potential security gaps. This includes regular security assessments, penetration testing, vulnerability scanning, and ongoing monitoring of critical systems and networks. Additionally, establishing key performance indicators (KPIs) and metrics to measure the effectiveness of cybersecurity controls and operations can guide continuous improvement efforts.

Compliance with regulations

Compliance with relevant cybersecurity regulations and standards is essential for NHS organisations. This includes adherence to the Data Protection Act, General Data Protection Regulation (GDPR), and other applicable frameworks. Regular assessments and audits should be conducted to ensure compliance and maintain a strong cybersecurity posture.



It is important to note that the target operating model for cybersecurity in the NHS should be adaptable to evolving threats, technological advancements, and organisational changes. Regular review, evaluation, and updates to the model will help ensure its continued effectiveness in mitigating cyber risks and safeguarding critical healthcare systems and data.

Contact us:

Rajvir Cheema
Partner, Digital Healthcare Advisory
KPMG in the UK
E: rajvir.cheema@kpmg.co.uk

Richard Krishnan
Partner, Technology and Cyber Risk
KPMG in the UK
E: richard.krishnan@kpmg.co.uk

Thomas Jordan
Cyber Senior Manager
KPMG in the UK
E: thomas.jordan@kpmg.co.uk

Find out more: home.kpmg/uk/cyberforhealth

kpmg.com/uk

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public

CREATE: CRT152957A I December 2023