Building a strong cyber strategy for NHS Trusts and Integrated Care Systems

In today's digital age, the healthcare sector, including NHS Trusts and Integrated Care Systems (ICSs), faces an ever-evolving landscape of cyber threats. To safeguard patient data, protect critical infrastructure, and ensure uninterrupted delivery of care, a robust cyber strategy is crucial. In this article, we will explore the key components of a good cyber strategy for NHS Trusts and ICSs.

Governance and leadership

A strong cyber strategy begins with robust governance and leadership. NHS Trusts and ICSs should establish clear lines of responsibility and accountability for cybersecurity. This includes designating a dedicated cybersecurity leader or team responsible for overseeing and implementing the cyber strategy. Leadership should prioritise cybersecurity at all levels, ensuring that it is integrated into the organisation's overall risk management framework.

Risk assessment and management

Comprehensive risk assessment is essential for identifying vulnerabilities and developing effective mitigation strategies. NHS Trusts and ICSs should conduct regular risk assessments to identify and prioritise potential threats and vulnerabilities. This includes assessing the security of systems, networks, and connected devices, as well as evaluating the impact of potential cyber incidents on patient care. Based on the assessment, organisations can develop risk management plans that address identified vulnerabilities and ensure timely response and recovery.

Security controls and technologies

Implementing strong security controls and technologies is a cornerstone of an effective cyber strategy. This includes deploying robust firewalls, intrusion detection and prevention systems, and anti-malware solutions. Access controls, including strong authentication mechanisms and role-based permissions, should be in place to limit unauthorised access to sensitive data and systems. Encryption should be utilised to protect data both at rest and in transit. Regular vulnerability assessments and penetration testing should be conducted to identify and address any security gaps.

Employee education and awareness

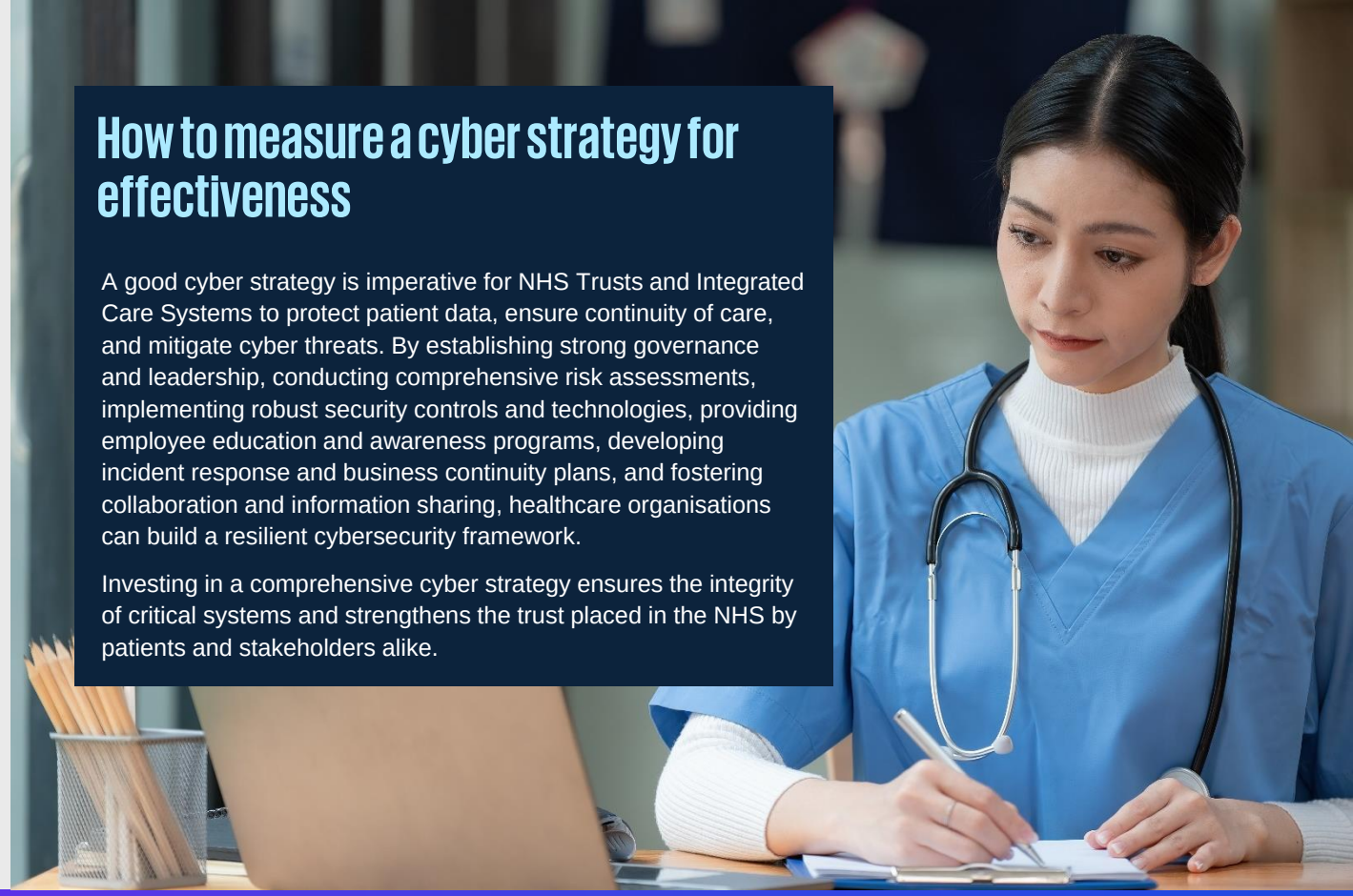
Human error remains one of the leading causes of cyber incidents. Therefore, comprehensive employee education and awareness programs are critical components of a robust cyber strategy. NHS Trusts and ICSs should provide regular training sessions to staff members, emphasising the importance of cybersecurity practices such as recognising and reporting phishing attempts, creating strong passwords, and adhering to safe browsing habits. Ongoing awareness campaigns can help ensure that all staff members understand their roles and responsibilities in maintaining a secure environment.

Incident response and business continuity

No cybersecurity strategy is complete without a well-defined incident response and business continuity plan. NHS Trusts and ICSs should establish procedures for detecting, reporting, and responding to cybersecurity incidents promptly. This includes defining roles and responsibilities, establishing communication channels, and coordinating with relevant stakeholders, such as regulatory authorities and incident response teams. Regular drills and simulations should be conducted to test the effectiveness of the plan and ensure that staff members are familiar with their roles during a cyber incident.

Collaboration and information sharing

Collaboration and information sharing play a vital role in enhancing cybersecurity within the healthcare sector. NHS Trusts and ICSs should actively engage with industry groups, government agencies, and peer organisations to share best practices, threat intelligence, and lessons learned from cyber incidents. Sharing information helps organisations stay abreast of emerging threats and enables collaborative efforts to counteract them effectively.



How to measure a cyber strategy for effectiveness

A good cyber strategy is imperative for NHS Trusts and Integrated Care Systems to protect patient data, ensure continuity of care, and mitigate cyber threats. By establishing strong governance and leadership, conducting comprehensive risk assessments, implementing robust security controls and technologies, providing employee education and awareness programs, developing incident response and business continuity plans, and fostering collaboration and information sharing, healthcare organisations can build a resilient cybersecurity framework.

Investing in a comprehensive cyber strategy ensures the integrity of critical systems and strengthens the trust placed in the NHS by patients and stakeholders alike.

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.

Document Classification: KPMG Public

CREATE: CRT152957A I December 2023