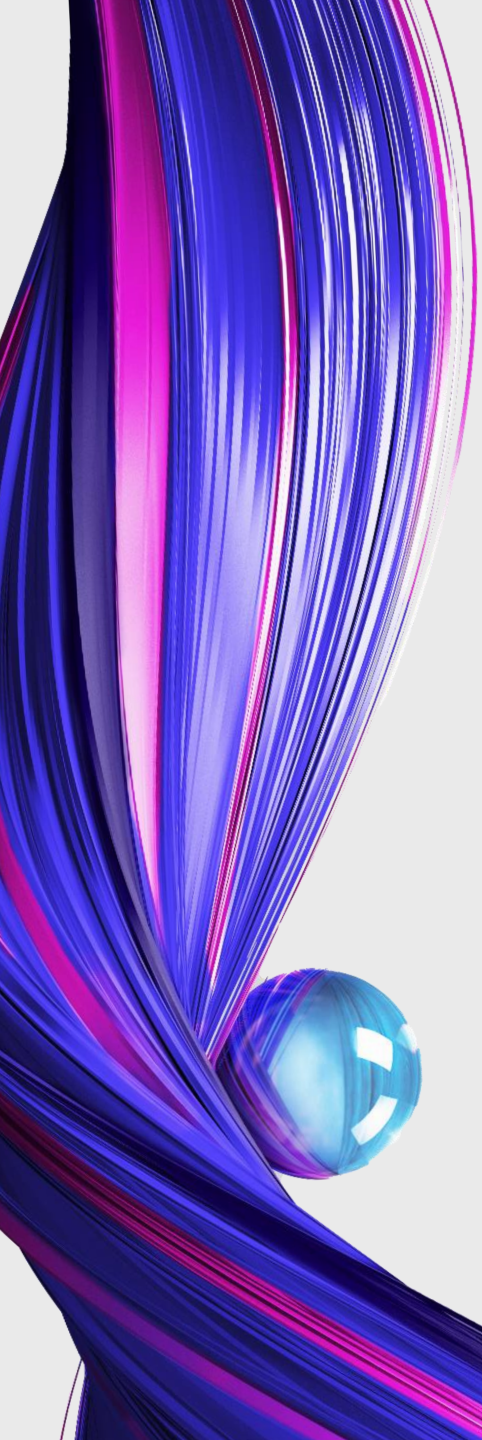


Adopt: Improve outcomes for patients and user satisfaction through data-driven insight

Safeguarding patient data in the digital age

Building a cyber secure and resilient healthcare system

In today's increasingly interconnected world, the healthcare sector faces unprecedented challenges when it comes to securing patient data and protecting critical infrastructure from cyber threats. With the digitisation of medical records and the adoption of connected devices, the potential for cyberattacks on healthcare systems has soared. According to recent statistics, cyberattacks targeting healthcare organisations have increased by a staggering 350% since 2017. In this article, we will explore essential steps healthcare organisations can take to create a cyber secure and resilient healthcare system.

Conduct a comprehensive risk assessment

Before implementing any cybersecurity measures, it is crucial for healthcare organisations to conduct a thorough risk assessment. This assessment should identify vulnerabilities in the network infrastructure, applications, and systems that store and process patient data. By understanding potential threats and their impact, organisations can prioritise their cybersecurity efforts effectively.

Establish a robust security framework

Healthcare organisations must establish a strong security framework that aligns with industry best practices. This includes implementing multi-factor authentication, encryption, firewalls, intrusion detection systems, and regular security patching. Additionally, all systems and devices must be kept up to date with the latest security patches and software updates to mitigate vulnerabilities.

Train and educate staff

Human error remains one of the most significant factors in cyber breaches. Healthcare organisations should invest in comprehensive training programs to educate employees about cybersecurity best practices, such as identifying phishing emails, using strong passwords, and recognising social engineering techniques. Regular training and awareness campaigns can significantly reduce the risk of internal security breaches.

Implement access controls and data privacy measures

To protect sensitive patient data, healthcare organisations must establish strict access controls. Implementing role-based access controls ensures that only authorised personnel can access and modify patient records. Additionally, healthcare providers should adhere to relevant data privacy regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), to safeguard patient information and maintain compliance.

Conduct regular vulnerability assessments and penetration testing

Regular vulnerability assessments and penetration testing help healthcare organisations identify weaknesses in their systems and networks. By simulating real-world cyberattacks, organisations can gauge their security posture and identify potential entry points for malicious actors. These assessments provide valuable insights into vulnerabilities and allow for proactive remediation to prevent future breaches.

Establish an incident response plan

Having a well-defined incident response plan is critical to minimising the impact of a cyberattack. Healthcare organisations should establish clear protocols for reporting, investigating, and containing security incidents promptly. This includes having a designated incident response team, developing communication strategies, and conducting regular drills to test the efficacy of the plan.

Summary of key considerations and actions for healthcare leaders:

In summary, creating a cyber secure and resilient healthcare system requires a multifaceted approach that addresses both technological and human factors. Healthcare organisations should take the following actions to strengthen their cybersecurity posture:

01

Conduct a comprehensive risk assessment to identify vulnerabilities.

02

Establish a robust security framework aligned with industry best practices.

03

Invest in staff training and education to mitigate human errors.

04

Implement access controls and data privacy measures to protect patient data.

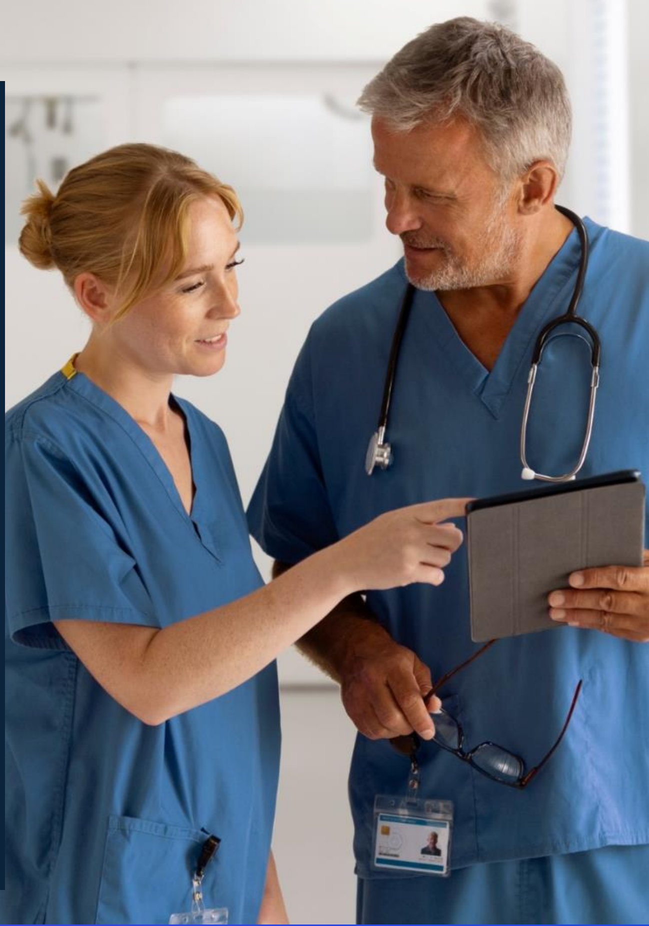
05

Regularly assess vulnerabilities and conduct penetration testing.

06

Develop and regularly test an incident response plan to minimise the impact of cyberattacks.

By implementing these actions, healthcare organisations can significantly enhance their ability to withstand cyber threats and safeguard patient data. Ultimately, a cyber secure and resilient healthcare system is crucial to preserving trust in the digital age and ensuring the well-being of both patients and healthcare providers.



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