cyberlab

Cyber Diagnosis: Navigating Cyber Security Challenges in Healthcare

Top 4 Cyber Threats to the Healthcare Sector and its Supply Chain

cyberlab

On-Demand

Cyber Diagnosis: Navigating Cyber Security Challenges in Healthcare

Supported by

SOPHOS FORESCOUT LOGPOINT SecurEnvoy

In this exclusive webinar hosted by CyberLab, in collaboration with industry-leading partners Sophos, Logpoint, Forescout, and SecurEnvoy, we explore how to safeguard healthcare organisations against cyber threats.

In this webinar, we cover:

- Industry Insight: Understanding the unique cyber security challenges faced by the healthcare sector compared to other industries, alongside the latest regulatory compliance requirements.
- Virtual Viruses, Real Solutions: Discover practical strategies and solutions from industry experts to enhance cyber security resilience and response capabilities.

Visit Cyberlab.co.uk or scan QR Code

Introduction

In an era where healthcare is increasingly reliant on digital technologies, the security of sensitive patient data and critical systems has never been more crucial.

Healthcare organisations are frequent targets for cyber criminals due to the wealth of personal and medical information they handle, often using legacy systems.

This whitepaper explores the evolving cyber threat landscape for healthcare organisations, identifies key security challenges, and outlines effective strategies to mitigate risks.

Contents:

Understanding the Threat Landscape

The 4 Most Prevalent Threats

Healthcare organisations are prime targets for cyber attacks due to the valuable information they hold, such as medical records, financial data, and intellectual property.

Given the estimated daily volume of 950,000 general practice appointments, 45,000 major AandE department visits, and 137,000 imaging procedures, the potential impact of a cyber attack on the health and social care sector is immense, both directly and indirectly.*

Ransomware

Ransomware is malicious software that encrypts critical data, disrupting operations until a ransom is paid. These attacks can severely impact the ability of healthcare providers to deliver timely and effective care.

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Case Study: Ireland Health Service Executive

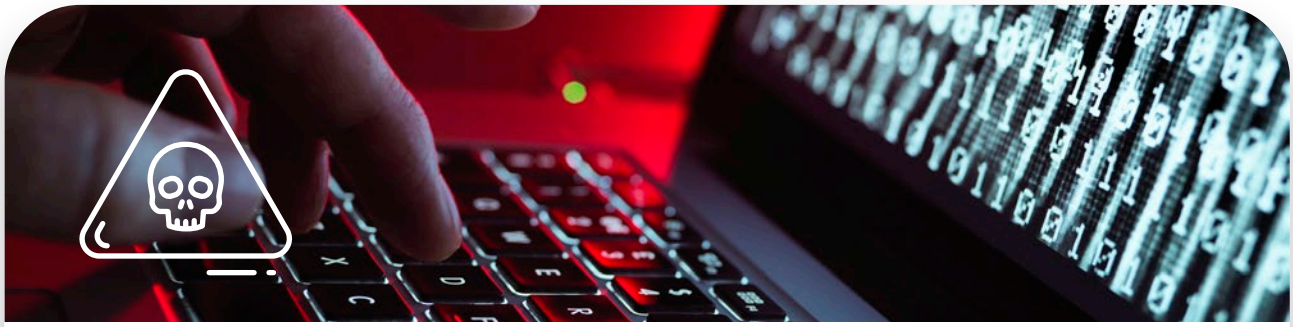
In 2021, the Health Service Executive (HSE) in Ireland experienced a significant ransomware attack that encrypted 80% of its IT environment. This incident hindered access to diagnostic tools and medical records, severely disrupting healthcare services nationwide. Outpatient clinics and other healthcare services were cancelled, resulting in an 80% reduction in medical appointments.

The financial repercussions were substantial, encompassing the immediate costs of the attack, recovery efforts, and the reconstruction of security systems. The HSE reported a revenue expenditure of €37 million and a capital expenditure of €14 million for 2021. While the total cost of the attack has yet to be fully determined, estimates suggest it will reach nearly €657 million over seven years to enhance cyber security measures*

*Source: A cyber resilient health and adult social care system in England: cyber security strategy to 2030 - GOV.UK (www.gov.uk)

Legacy Systems

Legacy systems in healthcare are a significant cyber security concern due to their outdated technology and lack of modern security features. These systems often operate on older, unsupported operating systems that do not receive regular security updates, making them vulnerable to cyber attacks.



Case Study: **WannaCry Attack, 2017**

Although not specifically aimed at the UK health sector, the NHS in England and Scotland was significantly affected by the WannaCry Attack due to many devices running supported but unpatched operating systems. This attack led to disruptions in at least 34% of NHS trusts in England, resulting in thousands of cancelled appointments and operations due to known and unfixed security weaknesses.

"The WannaCry cyber attack had potentially serious implications for the NHS and its ability to provide care to patients. There are more sophisticated cyber threats out there than WannaCry so the Department and the NHS need to get their act together to ensure the NHS is better protected against future attacks."

*Source: A cyber resilient health and adult social care system in England: cyber security strategy to 2030 - GOV.UK (www.gov.uk)

Phishing Attacks

Phishing attacks involve deceptive emails or messages that trick employees into revealing sensitive information or installing malware. Despite the growing prevalence and risks associated with phishing, only 18% of organisations have implemented phishing simulations to test and educate their staff.

Supply Chain Risk

Supply chain risk in healthcare organisations refers to the vulnerabilities introduced through third-party vendors and suppliers who provide critical services, equipment, and software. These external entities often have access to sensitive patient data and essential operational systems, making them potential entry points for cyber attacks.

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/
[2] Third-party cyber risks impact all organizations - Marsh

Navigating Cyber Security in Healthcare

Whilst cyber defences have undoubtedly strengthened over recent years, particularly following the WannaCry incident in 2017, healthcare organisations continue to grapple with significant cyber security challenges. It is vital for healthcare entities to embrace a proactive and thorough approach, prioritising the protection of critical systems against the prevailing risks.

Balancing Budget Constraints

Securing healthcare organisations involves a delicate balance between financial limitations and the need for robust cyber security measures. Healthcare providers must strategically allocate resources to address the most critical vulnerabilities without compromising patient care or operational efficiency.

Risk-Based Approach

Focus investments on critical assets and vulnerabilities identified through a thorough risk assessment. Prioritise resources based on the organisation's risk profile to address the most significant threats first.

Baseline Security Practices

Implement essential security measures such as regular patch management, strict access controls, and comprehensive employee training. These foundational practices create a robust security framework.

Assessing Security Controls

Healthcare organisations face unique cyber security challenges due to the sensitive nature of the data they handle and the complexity of their IT environments. To address these challenges, many healthcare providers leverage Microsoft for their extensive security capabilities. However, to maximise the effectiveness of these tools, it is crucial to ensure that security controls are both comprehensive and adaptable.

- Comprehensive Coverage: Coverage extends to endpoints, servers, and unmanaged IoT devices.
- Third-Party Integration: Microsoft tools should integrate well with third-party solutions for effective threat detection and response.
- Continuous Improvement: Regular assessments, updates, and training are necessary to stay ahead of emerging threats.
- Correct Configuration: Ensure that security tools are configured to align with healthcare-specific needs and regulatory standards.

Defence in Depth

Defence in depth is a cyber security strategy that involves deploying multiple layers of security controls to protect against various threats. This approach recognises that no single security measure is foolproof and aims to create redundancy and resilience by diversifying defence mechanisms.

Each layer acts as a barrier, mitigating the risk of successful cyberattacks and reducing their impact if one layer is compromised. By implementing defence in depth, organisations enhance their ability to detect, respond to, and recover from cyber incidents effectively.

Learn More about Defence in Depth >

10 Steps to Cyber Security

The UK's National Cyber Security Centre (NCSC) has developed a comprehensive guide, the "10 Steps to Cyber Security", aimed at helping organisations enhance their cyber security. The guidance outlines ten critical steps, ranging from establishing a risk management regime to securing the supply chain, each designed to mitigate risks and protect against potential cyber threats.

Understanding 10 Steps to Cyber Security

- Risk management
- Engagement and training
- Asset management
- Architecture and configuration
- Vulnerability management
- Identity and access management
- Data security
- Logging and monitoring
- Incident management
- Supply chain security

Understand your security risks and how to fix them!

Take our FREE Cyber Security Health Check

Completed alongside a CyberLab expert, the CyberLab Cyber Health Check is completely free and will review all the most relevant aspects of your security posture.

Following the 10 Steps to Cyber Security, we will assess your organisation across the ten key areas that should be considered to form a robust yet realistic cyber security strategy.

Our experts uncover your security risks and provide actionable insights to bolster your defences against future attacks.

Book Your Free SME Security Posture Assessment

Find out more at cyberlab.co.uk

Protecting Your Systems, Data and Patients

Not only do cyber threats affect your systems and data security, they can also affect patient outcomes.

Our range of healthcare security solutions have been developed to meet the security requirements of modern healthcare providers, and through years of experience with our healthcare clients.

We've put together these recommendations to ensure service availability, protect your systems and networks, and keep sensitive data safe.

Asset Management

Discover and classify all devices upon connection to your network, automatically evaluate their security posture and segment them appropriately.

Data Security

Enhance the security of sensitive data and ensure that only those with legitimate permissions are granted access.

Compliance

Enhance the security of sensitive data and confidently meet and surpass current and upcoming compliance requirements.

Malware and Ransomware

Leveraging AI to look for malicious behaviour patterns, next-gen anti-virus solutions detect novel malware with a high degree of success.

Email Security

Protect against email borne threats, preserve the flow of information and ensure secure communication with threat detection and prevention.

Data Control

Gain control over what is classified as sensitive data, what limitations are placed on it, where it's stored, and what happens if it is lost or stolen.

Cyber Security Solutions for Healthcare

Sophos Managed Detection and Response (MDR)

Used by healthcare organisations across the world, Sophos MDR integrates with your existing security investments and can be configured to provide full-scale incident response or to supply the accurate information needed to make security decisions.

Few organisations have the right tools, people, and processes in-house to manage their security program around-the-clock while proactively defending against new and emerging threats.

Sophos MDR is a fully-managed 24/7/365 threat hunting service delivered by specialists in detecting and responding to sophisticated cyber attacks.

Microsoft 365 Consultancy

Leverage our expertise with Microsoft consultancy services designed to help you make the most of your Microsoft investment, including MS Defender for Endpoint, 365 and Cloud, Device management via MS Intune, Identity and Access Management, Information Protection, Security Health Checks against CIS Control and Secure Score Improvement.

Forescout Asset Management and Security

As healthcare becomes more digital, an increasing number of IoT, OT, IT, and medical devices are connecting to healthcare networks. While this is a positive trend in many ways, it does increase cyber risk as more devices mean a bigger attack surface.

Forescout provides an intuitive platform to address the key areas of need in healthcare organisations today:

Lack of visibility: The inability to see many devices leads to blind spots and unknown devices on enterprise networks.

Default passwords: Critical-care devices using default credentials reside alongside other connected systems and can be manipulated by outsiders and used to spread malware.

Insufficient segmentation: Risky devices are left unchwecked, connecting and communicating with limited oversight, or none at all.

Un-agentable/unpatchable devices: Many IoT and IoMT devices can't be patched, and some critical-care systems can't be taken offline for patching.

CyberLab – Proud to Protect the Healthcare Sector

CyberLab look after over 150 public and private healthcare providers, working together to develop solutions that secure their sensitive data, meet compliance requirements, and ensure online threats don't compromise their operation.

Our range of security services and solutions have been developed to meet the requirements of the NHS Data Security and Protection Toolkit (DPST) and future-proofs against the NCSC's Cyber Assessment Framework (CAF).

NHS Trust

When this Head of IT at an NHS trust needed an independent security assessment to test the integrity of their Microsoft 365 infrastructure, they knew from experience that CyberLab was the right firm for the job.

"Having used CyberLab before in a previous Head of IT role, I had no hesitation in engaging them again to assist us with our security needs. Simply, I wouldn't use them if they didn't consistently deliver value."

– Head of IT, NHS Trust

Vaccination UK

The leading provider of in-school vaccinations came to CyberLab for help in securing their systems while undergoing a digital transformation.

"CyberLab were pivotal in helping Vaccination UK take a step forward into modernising our services, streamline our reporting and workforce, and assisting in rolling out a huge step change in how we deliver our services."

– James Hart, Head of Operations for NHS Services, Vaccination UK

Our People. Our Platform. Protects You.

CyberLab is a specialist cyber security company that provides a wide range of security solutions and services.

Your one-stop cyber security advisor, the CyberLab team is equipped with the right technology, knowledge, and expertise to help businesses of all sizes, including large public sector organisations.

By leveraging world-class technology, decades of experience, and our vendor partnerships, we have helped to secure thousands of organisations across the UK.

Our unique Detect, Protect, Support approach makes us the perfect partner to review and reenforce your cyber security defences.

Speak With an Expert

hello@cyberlab.co.uk | cyberlab.co.uk

Awards and Accreditations

CREST

VA | PEN TEST

IASME CONSORTIUM

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

cyberlab

cyberlab.co.uk