25/26 MIAA Audit Committee Insight

Non-Executive Director Briefing

Cyber Security

January 2026

miaa

1 Introduction

This briefing aims to help NHS Non-Executive Directors understand the importance of cyber resiliency, highlighting the risk and impact that a cyber security incident presents to patient care.

It is informed by NHS England's guide for Non-Executives (NEDs) and the National Cyber Security Centre (NCSC) board toolkit [1],[2].

> "Cyber is a tier one risk affecting organisations of all shapes and sizes. The NHS is clearly not immune, as has been made abundantly clear over recent years. These incidents have not only been costly but have had direct impact on patient safety and care. Boards throughout the NHS have a key role to play in safeguarding patients from this risk.
>
> **Dr Jamie Saunders, Non-Executive Chair of the NHS England Cyber Security Risk Committee**
>
> **NHS England Cyber security guide for non-executive directors**

This document outlines some key questions NEDs should consider asking about the protections and preparedness of their organisation to safeguard patient interests in the event of a severe cyber event.

2 Role of the NEDs

> Non-Executive Directors (NEDs) assist boards to provide independent oversight, governance, support decision making, and offer strategic direction/guidance to facilitate informed board decision making.
>
> Boards have ultimate accountability for overseeing and directing an organisation's security measures. Understanding your cyber risk approach will help you to do this.
>
> **NHS England Cyber security guide for non-executive directors**

[1] What cyber security is - NHS England Digital

[2] Cyber Governance Training - NCSC.GOV.UK

3 Background

NCSC's Annual Review 2025[3] has emphasized "*the importance of cyber resilience as a shared national priority, with an expanding threat landscape and a key priority of designing resiliency into critical systems*". NCSC advised that national significant incidents represent 48% of all incidents, which represents a significant increase on the previous year. Of those incidents,18 or 4% were categorised as being highly significant. An increase for the third year.

A nationally significant incident covers incidents in the upper 2 categories in the NCSC and UK law enforcement categorisation model.

- **Category 1** – National cyber emergency - A cyber-attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life.
- **Category 2** – Highly significant incident - A cyber-attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.
- **Category 3** – Significant incident - A cyber-attack which has a serious impact on a large organisation or on wider/local government, or which poses a considerable risk to central government or UK essential services.

> *"A key challenge … is ensuring board members can communicate effectively about cyber risk. Unlike financial or legal risk, cyber risk is not always on the board's agenda. Leaders are fluent in the language of revenue, liability, and shareholder value, but cyber security is often framed in technical terms that feel disconnected from business strategy. ….. cyber risk must be translated into business risk, so that board members can approve necessary mitigations."* [1]

The impact of cyber incidents has become more evident in recent times. This has led to greater impacts being seen across Trusts and directly impacting patient safety. A recent cyber incident highlighted at a GARNet event[4] the risk:

- It's **NOT** a technology risk
- It's **NOT** a compliance risk
- It **IS** a clinical risk
- It **IS** a financial risk
- It **IS** an operational risk
- It **IS** a reputational risk.

[3] NCSC Annual Review 2025 - NCSC.GOV.UK

[4] GARNET Information Governance event, MIAA presentation, 9th September 2025

The **Synnovis** cyber incident context:

- Provide pathology services to a number of hospitals in the south
- Ransomware attack on 3rd June 2024
- Data stolen
- Systems offline
- Service capacity severely reduced
- GP blood testing across southeast London not resumed until September 2024
- Blood transfusion IT systems at Guy's and St Thomas' were restored in October 2024

Post incident analysis of this incident:

- **One patient death directly attributed to the incident**
- At least 2 patients suffered long-term or permanent damage to their health
- 11 cases of moderate harm
- 120 cases of low harm
- 10,152 acute outpatient appointments postponed
- 1,710 elective procedures postponed
- Exfiltration and publication of circa 400gb of sensitive patient information
- Response and recovery cost of circa £33m were incurred
- A large fine is likely in due course (Advanced were fined £3m as a result of their cyber incident)

4 Role of Audit and the Data Security Protection Toolkit (DSPT)

NCSC's Cyber Assurance Framework (CAF) underpins the new Data Security Protection Toolkit (DSPT) requirements and promotes an understanding of which services are critical to the organisation, how risks are identified and managed, and how services are maintained and recovered during disruption. NCSC also launched the Cyber Resilience Audit (CRA) scheme providing a network of audit providers, of which MIAA is a member, committed to high standards of security and independence. It launched the scheme to ensure organisations can undergo independent cyber audits based on the CAF.

- The DSPT was strengthened in September 2024 and aligned with the CAF. This was a commitment made in the Department of Health and Social Care cyber security strategy for Health and Social Care to 2030, to enhance the cyber security assurance of government organisations, as part of the underpinning 5 pillars of the strategy.

This document outlines the steps organisations should consider when reviewing cyber security from a Non-Executive Director perspective

.

5 Cyber Security – Steps to Consider

Questions to Ask Yourself

Knowledge and Understanding

- Do I know and understand the cyber risks of my organisation?
- Do I understand the board's cyber updates, briefings or papers? If you are currently not in receipt of these, you should make a request.
- Outside of board meetings, do I regularly speak to the members accountable for cyber risk – SIRO (Senior Information Responsible Officer), Chief Information Officer (CIO) or Chief Information Security Officer (CISO) to improve my understanding of the organisation's threat profile, controls and processes?

Governance

- Do I know who is accountable for cyber risks on the board and who is responsible for managing them in the organisation?
- Am I confident there is sufficient segregation between those accountable and those making decisions about the technological direction of the organisation?
- Am I aware that technical staff may be accepting risk on behalf of the board, when they do not have the delegated authority to do so?

Briefings

- Are the updates and briefings tailored to enable the board to understand the risk to their strategic objectives?
- Are cyber risk management strategies presented in a way that facilitate informed financial spending discussions at strategic level?
- Do briefings cover the basic areas outlined in the Government's 10 steps to cyber security guidance?

Risk Management

- Do I regularly discuss the level of cyber risk and how much is the organisation prepared to invest to manage that risk?
- Am I being offered choices or options to manage cyber risk?
- Do I understand the cyber risk landscape/posture of the organisation and how much untreated or residual risk we are holding?
- How confident am I that when a cyber incident occurs everyone knows their role and responsibilities including escalation?

Questions to the Board

Governance

- Who manages the organisation’s cyber security risk on a day-to-day basis?
- Who is the Senior Information Risk Owner (SIRO)? (All NHS organisations must have a SIRO to take responsibility for Information Assurance (IA) issues).
- Is there an executive and non-executive lead for cyber security on the board?
- Does the appropriate governance structure exist between the executive team and the cyber security function?
- If cyber security is considered in a board sub-committee, such as the audit and risk committee, how much time and cyber security expertise does it have to examine cyber security and how effective is the governance?

Briefings

- When did the board last receive a briefing on the cyber security threat to healthcare?
- When did the board last participate in cyber security awareness activities?

Risk Management

- Has the executive team identified the most critical assets and data?
- How is cyber security risk integrated into wider business risks?
- How frequently does the board review cyber security risk and is this appropriate to the increased cyber risk?
- How are risks presented in performance dashboards?
- Has the board reviewed the data from the Data Security and Protection Toolkit (DSPT) to inform board risk discussion?
- How prepared is the Board to respond to an incident where cyber is the cause?
- In the event of a cyber security incident, how can the board ensure critical services can be maintained over a potentially extended period?

Questions for the Board to Ask

Technology

- How do we defend our organisation against common and well-known attack techniques, such as phishing attacks?

Note: Phishing is one of the most likely ways by which an attacker will first gain access to an organisation.

- How do we ensure the security of administrator, privileged or high access accounts and are they separated from 'day to day' accounts?

Note: Attackers will wish to compromise administrator accounts because they hold elevated access. These accounts must be given additional protection.

- Do digital teams have a lifecycle management for technology to ensure we are not running out-of-date software, which would lead to vulnerability?
- How do we make sure our partners and suppliers protect the information we share with them?
- How do we understand the links between our suppliers and the key systems and services they provide to us? What are our key suppliers doing to protect their own systems, so they can provide our organisation with resilient services?

Note: All NHS organisations will be dependent on third parties as part of their supply chain: this will mean that data is shared, and there may be direct connectivity. Steps need to be taken to minimise the risk that these connections represent

- Suppliers of digital services – how do we ensure that other critical supply chains (for example, not only digital supply chains) are resilient to cyber disruption? This may overlap with the assurances required to ensure we are meeting our GDPR data controller obligations when sharing personal data to external data processors and may extend to delivery of services as well as data protection and information security.
- Do we have multi-factor authentication (MFA) securing all access into our data, information and systems from outside of our internal network?

Note: Attackers exploit any weaknesses in access control measures (passwords etc). Implementing measures such as two-factor or multi-factor authentication (2FA or MFA) can reduce this risk.

People

- Thinking across the organisation, do you feel that there is a positive, negative or indifferent cyber security culture?
- When was the last cyber security awareness campaign for our organisation? What did we do and what did we do with our findings?

Note: NHS England has produced security awareness materials that have been widely tested and are available for your organisation to quickly deploy, saving time and money for your organisation.

- Do you have a dedicated and skilled team responsible for cyber security?

Note: Recruiting and retaining cyber security professionals is very challenging. You may need to consider collaborating with other NHS organisations or outsourcing some security functions.

Questions for the Board to Ask

Resilience

- Are backups validated and assured when taken, can they be relied upon when needed? Also, are backups and their data protected from attackers who may wish to delete, change or steal them?

Note: Attackers who deploy ransomware seek out back-ups to disable or delete. Therefore, having a secure off-line back-up is essential if an organisation is going to be able to recover quickly from a ransomware attack.

- Are incident management and business continuity plans in place and when were they last reviewed and exercised?
- Do our incident management and business continuity plans include cyber risk scenarios, and ensure critical services can be maintained over a potentially extended period?

Regulation

- Do we fully understand our governance, legislative and regulatory responsibilities around cyber security and the potential penalties for non-compliance?
- Have there been any recent changes to legislation/regulations that we need to be aware of?

Understanding your strategies as a board member for managing cyber risk

- Is cyber security risk on the BAF (Board Assurance Framework)?
- What are your key cyber security risks and how they are being prioritised and mitigated?
- Who is accountable for cyber security and who is responsible? Where are decisions made and recorded?
- Which data and systems do you care about most and have any risk assessments been carried out?
- What is your risk appetite and is it documented?
- Is it clear how the organisation maintains critical services and protects patient interests in the event of a prolonged cyber event?

7 Key References

1. 10 Steps to Cyber Security - NCSC.GOV.UK -

2. Data Security and Protection Toolkit

3. NCSC assured cyber security training for NHS boards - NHS England Digital

4. Cyber security guide for non-executive directors - NHS England Digital, July 2025

5. It's time to act - NCSC Annual Review 2025

6. Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT) - NHS England Digital

7. Cyber security strategy for health and adult social care to 2030 - NHS England Digital

8. GARNET Information Governance event, MIAA presentation, 9th September 2025

Find out more:

If you have any queries or feedback on this briefing, please contact:

Paula Fagan, Head of Technology Risk

Email: paula.fagan@miaa.nhs.uk

Catherine Watts, Principal Digital Risk Consultant

Email: catherine.watts@miaa.nhs.uk

miaa