LITERATURE ANALYSIS AND REPORT OUTLINE

Methodology

The literature reviewed was sourced using an integrative approach to gather both academic and grey literature within the last 5 years (2020-2025). This method enabled a broader search, providing a wider variety of sources to critique the NHS cyber incidents and their non-technical causes.

Search Strategy: Literature was sourced from academic databases (google scholar, PubMed, ScienceDirect) using Boolean combinations of keywords including: ("NHS" OR "healthcare") AND ("cybersecurity" OR "cyber incidents") AND ("non-technical factors" OR "human errors" OR ("governance" OR "ISM practices") AND ("2020-2025").

Analysis Process: A thematic approach identified recurring themes, including human errors, governance failures, and ISM weaknesses, which were mapped to NHS case studies to ensure contextual relevance. This provided a more organised analysis, ensuring relevant topics weren't missed. Limitations include publication bias and exclusion of pre-2020 literature providing insights into ISM policy evolution.

Literature Analysis

This analysis explores rising NHS cyber incidents, focussing on non-technical ISM factors. Recent incidents, such as the Synnovis ransomware attack (NHS England, 2024), highlight system vulnerability caused by weakness in governance, human behavior, and organizational culture rather than technical tools. The critique examines literature evidence of these factors, highlighting biases, gaps and implications for NHS's cybersecurity.

Human Error Factors

The Mimecast State of Human Risk 2025 report identifies human risk as the primary cyber security challenge, with insider threats and credential misuse driving breaches (Sedova, 2025). A 2025 spear-phishing attack on the NHS exploited overworked staff to disclose sensitive data (ProtekCyber Team, 2025). While literature often blames human error, I argue this is biased and a cover for the organizational failures. As Tonkin (2024) argues, human error is often due to an individual failing, rather than weakness within the system.

The Mimecast survey shows 94% of organisations, including healthcare, struggle to ensure employees adhere to security protocols, due to insufficient training. Ewoh et al.'s (2025) sociotechnical review of 1,375 studies supports this, highlighting that budget constraints and lack of skilled support increase self-related errors. In the NHS's high-pressure environment, long shifts and operational stress raise susceptibility to phishing and social engineering attacks.

I argue that the literatures focus on human error as a primary cause is not only biased but also counterproductive. It diverts attention from the NHS's failure to provide adequate training, clear policies, and sufficient resources, which increases employee vulnerability. For example, understaffing and budget constraints limit time and resources available for cybersecurity awareness, making organizational failings the cause of human error. Addressing these systemic issues would be more effective than focusing on human error alone.

Governance and ISM Weaknesses

Robust ISM requires effective governance, yet NHS cyber governance remains inconsistent. Imperial College London (Ghafur et al., 2020) found significant weakness in ISM policy implementation across

NHS trusts. Dobski (2024) notes that adopting frameworks like ISO/IEC 27001 enhances security by providing a clear structured approach to policy and risk mitigation. However, because these standards are non-mandatory, their implementation would not be effective in the NHS, due to its decentralised structure, limiting its effectiveness. Furthermore, with trusts lacking accountability and proper incident management procedures, it could create further governance gaps that attackers exploit, as these frameworks risk becoming a "tick box" exercise rather than a driver of change.

The 2024 Synnovis ransomware attack further illustrates these governance weaknesses (Uk Parliament, 2025). Despite failed technical defences, delayed incident response and poor communication between trusts highlighted leadership and policy inconsistencies. Although the literature acknowledges these weaknesses, it rarely addresses their root cause and this attack has shown that technology alone cannot compensate for weak governance.

Conclusion

The literatures bias towards attributing cyber incidents to human error overlooks the deeper governance and organisational failings causing the NHS cybersecurity weakness. While frameworks like ISO/IEC 27001 offer strong theoretical guidance, their non-compulsory status and uneven implementation across decentralised NHS trusts limit their practical impact. Much of the existing literature reviewed acknowledges vulnerabilities but doesn't address systemic issues that prevents effective ISM across the NHS.

Report Outline and Structure

The report addresses the non-technical vulnerabilities in NHS cybersecurity, focusing on weak governance and ISM practices that were identified in the literature analysis. Despite literatures bias towards human error, the report will argue that insufficient training, unclear policies and resource constraints are the root causes. The core direction of the report will follow this, proposing a structured improvement plan to enhance NHS resilience through robust policies, training, and compliance. The structure includes:

1. **Introduction:** Outlines rising cyber threats, explains the report's aim to address non-technical vulnerabilities, and details the methodology guiding the report.
2. **Incident Analysis:** Examines recent NHS cyber incidents, such as the Synnovis ransomware attack, alongside comparable attacks in other organisations, highlighting operational impacts and linking staff errors to governance and ISM weaknesses.
3. **Asset and Risk Analysis:** Identifies physical and non-physical NHS assets, assesses potential threats, and provides mitigation strategies for key risks like phishing, data misuse and governance failures.
4. **Security Policy:** Outlines a security policy that defines objectives, clarifies staff roles aligned with ISO/IEC 27001 principles, and recommends best practices to mitigate identified risks.
5. **Training Plan:** Presents a training and awareness plan that outlines objectives, target staff groups, training methods and evaluation metrics to strengthen human behaviour.
6. **Legal Analysis:** Analyses relevant legislation, including GDPR and the Data Protection Act, explaining compliance requirements and non-compliance risks.
7. **Conclusion:** Summarises key findings and provides recommendations to ISM and address systemic non-technical risks within the NHS.

Table of Contents

Bibliography

Tonkin, T. (2024, December 6). *Cybersecurity: Cracks in the system*. The Doctor (BMA). Retrieved October 22, 2025, from https://thedoctor.bma.org.uk/articles/health-society/cybersecurity-cracks-in-the-system/

Ghafur, S., Fontana, G., Martin, G., Grass, E., Goodman, J., & Darzi, A. (2020). *Cybersecurity in health: A global threat to health systems*. Imperial College London, Institute of Global Health Innovation. Retrieved October 22, 2025, from https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf

Sedova, M. (2025, March 11). *The state of human risk*. *Mimecast*. Retrieved October 22, 2025, from https://www.mimecast.com/blog/the-state-of-human-risk/

Ewoh, P., Vartiainen, T., & Mantere, T. (2025, October 15). *Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: Scoping review*. *Journal of Medical Internet Research*. Retrieved October 22, 2025, from https://doi.org/10.2196/75584

NHS England. (2024, June 21). *Synnovis cyber attack – statement from NHS England*. Retrieved October 22, 2025, from https://www.england.nhs.uk/2024/06/synnovis-cyber-attack-statement-from-nhs-england/

Synnovis. (2024, July 1). *Cyberattack update – 01 July 2024*. Retrieved October 22, 2025, from https://www.synnovis.co.uk/news-and-press/cyberattack-update-01-july-2024

Dobski, P. (2024). Information security management in the operations of healthcare entities. *Scientific Papers of Silesian University of Technology Organization and Management Series, 192*. Retrieved October 22, 2025, from https://doi.org/10.29119/1641-3466.2024.192.11

ProtekCyber Team. (2025, August 16). *NHS data breach*. *Protek Cyber*. Retrieved October 22, 2025, from https://protekcyber.co.uk/blog/nhs-data-breach/

UK Parliament, Committee of Public Accounts. (2025, May 9). *Government cyber resilience: Twenty-Fourth Report of Session 2024–25*. Retrieved October 22, 2025, from https://publications.parliament.uk/pa/cm5901/cmselect/cmpubacc/643/report.html

Appendix

Student Declaration of AI Tool use in this Assessment

Solo Work	**S1 - Generative AI tools have not been used for this assessment.**	☐
Assisted Work	**A1 – Idea Generation and Problem Exploration** Used to generate project ideas, explore different approaches to solving a problem, or suggest features for software or systems. Students must critically assess AI-generated suggestions and ensure their own intellectual contributions are central.	☐
	A2 - Planning & Structuring Projects AI may help outline the structure of reports, documentation and projects. The final structure and implementation must be the student's own work.	☐
	A3 – Code Architecture AI tools maybe used to help outline code architecture (e.g. suggesting class hierarchies or module breakdowns). The final code structure must be the student's own work.	☐
	A4 – Research Assistance Used to locate and summarise relevant articles, academic papers, technical documentation, or online resources (e.g. Stack Overflow, GitHub discussions. The interpretation and integration of research into the assignment remain the student's responsibility.	☒
	A5 - Language Refinement Used to check grammar, refine language, improve sentence structure in documentation not code. AI should be used only to provide suggestions for improvement. Students must ensure that the documentation accurately reflects the code and is technically correct.	☒
	A6 – Code Review AI tools can be used to check comments within the code and to suggest improvements to code readability, structure or syntax. AI should be used only to provide suggestions for improvement. Students must ensure that the code accurately reflects their knowledge and is technically correct.	☐
	A7 - Code Generation for Learning Purposes Used to generate example code snippets to understand syntax, explore alternative implementations, or learn new programming paradigms. Students must not submit AI-generated code as their own and must be able to explain how it works.	☐
	A8 - Technical Guidance & Debugging Support AI tools can be used to explain algorithms, programming concepts, or debugging strategies. Students may also help interpret error messages or suggest possible fixes. However, students must write, test, and debug their own code independently and understand all solutions submitted.	☐
	A9 - Testing and Validation Support AI may assist in generating test cases, validating outputs, or suggesting edge cases for software testing. Students are responsible for designing comprehensive test plans and interpreting test results.	☐
	A10 - Data Analysis and Visualization Guidance AI tools can help suggest ways to analyse datasets or visualize results (e.g.	☐

	recommending chart types or statistical methods). Students must perform the analysis themselves and understand the implications of the results.	
	A11 - Other uses not listed above Please specify:	☐
Partnered Work	**P1 - Generative AI tool usage has been used integrally for this assessment** Students can adopt approaches that are compliant with instructions in the assessment brief. Please Specify:	☐

Please provide details of AI usage and which elements of the coursework this relates to: Used to summarise articles and to check spelling/grammar, refine language and improve sentence structure within literature analysis, methodology and report outline.

I understand that the ownership and responsibility for the academic integrity of this submitted assessment falls with me, the student.	☒
I confirm that all details provide above are an accurate description of how AI was used for this assessment.	☒