**Unit 2: Research Questions, the Literature Review, and the Research Proposal**

**Literature Review and Research Proposal Outlines**

**1. What is the focus and aim of your review? Who is your audience?**

The review will focus on the financial impact of ransomware and malware on the healthcare sector. It will examine the economic challenges posed by cyber threats and highlight the urgent need for robust cybersecurity measures in healthcare settings. The intended audience includes healthcare administrators, policymakers, cybersecurity professionals, researchers in healthcare informatics, and other stakeholders in the healthcare industry.

**2. Why is there a need for your review? Why is it significant?**

Cyber-attacks on healthcare systems are increasingly frequent and sophisticated, causing substantial financial repercussions and disrupting operations. Understanding these financial impacts is crucial for healthcare professionals to implement effective cybersecurity measures. This review will underscore the pressing need for enhanced cybersecurity, guide policy and decision-making, and contribute to the broader discourse on healthcare cybersecurity.

**3. What is the context of the topic or issue? What perspective do you take? What framework do you use to synthesise the literature?**

The context involves the growing digitalisation of healthcare services and the accompanying rise in cyber threats targeting this sector. The review will cover significant ransomware and malware attacks on healthcare providers. It will adopt a financial perspective, analysing the economic impact of cyber-attacks on healthcare providers. The literature will be categorised into sections covering the nature of malware and ransomware, short-term and long-term financial impacts, case studies, mitigation and prevention strategies, and emerging trends.

**4. How did you locate and select sources for inclusion in the review?**

Sources will be located through academic databases such as PubMed and Google Scholar, as well as industry reports, whitepapers, and official documents from regulatory bodies. Priority will be given to recent sources from the past few years to ensure relevance and accuracy.

**5. How is your review structured?**

The review will be structured as follows:

* **Introduction**
* **Background on Ransomware in Healthcare**
* **Financial Impact on Healthcare Providers**
* **Case Studies of Financial Impact in Specific Attacks**
* **Mitigation and Prevention Strategies**
* **Conclusion**

**6. What are the main findings in the literature on this topic?**

Ransomware and malware attacks result in significant financial losses due to ransom payments, operational downtime, data recovery costs, legal fees, and increased insurance premiums. Long-term impacts include diminished patient trust, reputational damage, regulatory fines, and higher insurance costs. Effective mitigation strategies include regular software updates, employee training, advanced security technologies, and comprehensive incident response plans.

**7. What are the main strengths and limitations of this literature?**

* **Strengths**: The literature provides detailed analyses of financial impacts, practical case studies, and a range of mitigation strategies. It also emphasises the importance of regulatory compliance and government support.
* **Limitations**: There is a lack of standardised metrics for measuring financial impact, limited longitudinal studies on long-term effects, and potential biases in industry reports. Additionally, the rapidly evolving nature of cyber threats means that some information may become outdated quickly.

**8. Are there any discrepancies in this literature?**

Different sources report varying estimates of financial losses due to differences in methodologies and scope. There are also discrepancies in the reported effectiveness of certain mitigation strategies and the role of cyber insurance in fully covering financial losses.

**9. What conclusions do you draw from the review? What do you argue needs to be done as an outcome of the review?**

The financial impact of ransomware and malware on the healthcare sector is substantial, and it needs significant investments in cybersecurity. Both short-term and long-term financial repercussions highlight the need for proactive strategies. Healthcare providers should prioritise investments in advanced security technologies and employee training. Governments and regulatory bodies should offer increased support and resources. Further research is needed to develop standardised metrics for financial impact and to explore the long-term effects of cyber-attacks.