Consequences:

1. Operational Downtime:

Severe disruptions will cause delays in service, reductions in productivity, and losses for MASE Inc.; this may also affect the supply chain.

2. Data Leak/Breach:

The company's and customers' sensitive data may be jeopardized, serving as a conduit for financial fraud, theft of intellectual property, and possible legal complications, including financial fines.

3. Reputational Damage:

If the company cannot deliver services, it will affect consumer trust or public credibility. There will be negative press and this may lead to a permanent brand dent.

4. Financial Losses:

Some of the costs involved include paying the ransom, fines due to non-compliance with laws, recovery measures, and loss of business opportunities in both the near and long term, and increased insurance premiums.

5. Noncompliance with Regulations:

Poor compliance with legal requirements to protect data entails significant fines, sanctions, and enhanced scrutiny, which may disrupt operations.

6. Intellectual Property Theft:

Loss of proprietary data leads to lost competitive advantage and innovation because it weakens market position.

7. Insider Threats:

Carelessness or intentional decisions by insiders, such as employees, can lead to data breach compromises and system sabotage.

Overview of Appendices

Appendix A: Case study on NHLS Cyber Security Incident with event timeline and outcomes.

Appendix B: Cybersecurity tool and service providers recommended for MASE Inc.

Appendix C: Employee Cybersecurity Training - program plan detailing modules and assessment dates.

Appendix D: Incident response plan template covering the major steps that allow a determination of if cybersecurity incidents are detected, contained, and eradicated, and if recovery from them has taken place.