QUESTION No. 6

### Explanation Supporting Notes

#### Information Source(s) Used:

1. **Orca Security Blog**
   * **Type**: Website
   * **Key Themes**: Cloud security risks, weak password risks, mitigation strategies.
   * **Source**: [Orca Security Blog](https://orca.security/resources/blog/weak-host-password/)
2. **eSecurity Planet**
   * **Type**: Website
   * **Key Themes**: Cloud storage security issues, encryption methods, data breaches.
   * **Source**: [eSecurity Planet](https://www.esecurityplanet.com/cloud/cloud-storage-security-issues/)
3. **GlobalSign Blog**
   * **Type**: Website
   * **Key Themes**: Risks of outdated encryption, updating cryptographic protocols.
   * **Source**: [GlobalSign Blog](https://www.globalsign.com/en/blog/security-risks-outdated-encryption)
4. **Checkpoint Cyber Hub**
   * **Type**: Website
   * **Key Themes**: Phishing attacks, ransomware, insider threats.
   * **Source**: [Checkpoint Cyber Hub](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/)
5. **XenonStack Blog**
   * **Type**: Website
   * **Key Themes**: Insider threats, unauthorized access, data leaks.
   * **Source**: [XenonStack Blog](https://www.xenonstack.com/blog/insider-threats/)
6. **Palo Alto Networks Cyberpedia**
   * **Type**: Website
   * **Key Themes**: Denial of Service (DoS) attacks, system overload, service disruption.
   * **Source**: [Palo Alto Networks Cyberpedia](https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos)
7. **NCSC Reports**
   * **Type**: Government Reports
   * **Key Themes**: Application store threats, cyber threats to sports organizations.
   * **Source**: [NCSC Report on Application Stores](https://www.ncsc.gov.uk/report/threat-report-on-application-stores)
   * **Source**: [NCSC Report on Sports Organisations](https://www.ncsc.gov.uk/report/the-cyber-threat-to-sports-organisations)
8. **Advisera Blog**
   * **Type**: Website
   * **Key Themes**: International cyber security standards, ISO 27001, COBIT, BS 25999.
   * **Source**: [Advisera Blog](https://advisera.com/27001academy/knowledgebase/information-security-business-continuity-standards/)

#### Key Themes Identified:

1. **Common Cyber Threats**
   * Weak Passwords
   * Phishing Attacks
   * Ransomware
   * Insider Threats
   * Denial of Service (DoS) Attacks
2. **Risk Mitigation Strategies**
   * Implementing strong password policies.
   * Using encrypted password managers.
   * Regularly updating cryptographic protocols.
3. **Recent Cyber-Attacks**
   * Malware in application stores.
   * Cyber threats to sports organizations.
   * Business Email Compromise (BEC)
   * Cyber-enabled fraud
4. **Legislative Changes and Standards**
   * National Cyber Security Strategy 2016-2021
   * General Data Protection Regulation (GDPR)
   * Network and Information Systems Regulations (NIS)
   * International Standards (ISO 27001, ISO 27002, COBIT, BS 25999)

**Explanation:**

In the compilation of the notes for the assignment on the Cyber Security Strategy for Logistics Company, identification and understanding of the most relevant cyber threats and mitigation strategies were key. Key themes were drawn from a number of reputable sources, which included blogs and government reports, through to cybersecurity websites. This paper presented the detailed explanation for all these threats, their potential impact, and the legislative framework governing practices in the same.

This information is cross-checked against several sources for its reliability. For instance, the facts concerning phishing attacks are checked against sources like Checkpoint Cyber Hub and Phriendly Phishing, which are considered to be authoritative concerning their insights into cybersecurity issues. Similarly, insights into outdated encryption methods have been supported through eSecurity Planet and GlobalSign Blog.

This rigorous approach underpinned the comprehensiveness and reliability of the notes and provided a sound foundation for the assignment. Probably in the future, the use of other supporting materials, like academic articles or books of repute, would help further in getting a deeper understanding of the subject matter.

### References List:

* Orca Security Blog: [Orca Security Blog](https://orca.security/resources/blog/weak-host-password/)
* eSecurity Planet: [eSecurity Planet](https://www.esecurityplanet.com/cloud/cloud-storage-security-issues/)
* GlobalSign Blog: [GlobalSign Blog](https://www.globalsign.com/en/blog/security-risks-outdated-encryption)
* Checkpoint Cyber Hub: [Checkpoint Cyber Hub](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/)
* XenonStack Blog: [XenonStack Blog](https://www.xenonstack.com/blog/insider-threats/)
* Palo Alto Networks Cyberpedia: [Palo Alto Networks Cyberpedia](https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos)
* NCSC Report on Application Stores: [NCSC Report](https://www.ncsc.gov.uk/report/threat-report-on-application-stores)
* NCSC Report on Sports Organisations: [NCSC Report](https://www.ncsc.gov.uk/report/the-cyber-threat-to-sports-organisations)
* Advisera Blog: [Advisera Blog](https://advisera.com/27001academy/knowledgebase/information-security-business-continuity-standards/)