1. **Data security only protects data from unauthorized access, not from corruption or loss.** (False)
2. **A data breach can lead to financial loss, legal trouble, and reputational damage.** (True)
3. **EDM stands for Electronic Data Management.** (False) *(It stands for Enterprise Data Management.)*
4. **Data integrity ensures that data is not altered without authorization.** (True)
5. **Ransomware attacks do not involve hackers demanding payment to release locked data.** (False)
6. **GDPR is a data protection law that applies only to businesses in the U.S.** (False) *(It applies to businesses handling EU citizen data.)*
7. **Phishing attacks often use fraudulent emails to trick employees into revealing credentials.** (True)
8. **Encryption helps protect data by converting it into unreadable code for unauthorized users.** (True)
9. **Yahoo’s data breach affected only a few thousand accounts.** (False) *(It affected 3 billion accounts.)*
10. **A strong data security strategy includes regular backups to recover lost data.** (True)
11. **Insider threats come only from hackers outside the organization.** (False) *(They can come from employees or contractors too.)*
12. **Multi-Factor Authentication (MFA) requires only a password to secure an account.** (False) *(It adds extra security layers.)*
13. **HIPAA is a U.S. law that protects health-related data.** (True)
14. **The Facebook-Cambridge Analytica scandal led to stricter data privacy regulations.** (True)
15. **Once a company sets up a security policy, it does not need to be updated regularly.** (False) *(Security policies should be continuously updated.)*

Multiple choice

1. **What is the main goal of data security?**  
   a) To make data accessible to everyone  
   b) To protect data from unauthorized access, corruption, or loss  
   c) To delete unnecessary data regularly  
   d) To store data in multiple locations  
   **(Answer: b)**
2. **Which of the following is NOT a common cyber threat?**  
   a) Phishing  
   b) Data Encryption  
   c) Ransomware  
   d) Insider Threats  
   **(Answer: b)**
3. **Which regulation protects consumer data rights in California?**  
   a) GDPR  
   b) HIPAA  
   c) CCPA  
   d) ISO 27001  
   **(Answer: c)**
4. **What is the purpose of access controls in data security?**  
   a) To allow unrestricted access to data  
   b) To restrict who can view or modify data  
   c) To delete unused data  
   d) To back up data automatically  
   **(Answer: b)**
5. **Which of the following is an example of a high-profile data breach?**  
   a) Google Cloud Expansion  
   b) Yahoo Breach (2013-2014)  
   c) Tesla’s self-driving technology release  
   d) Apple launching Face ID  
   **(Answer: b)**
6. **What is one way businesses can prevent cyber threats?**  
   a) Ignoring security updates  
   b) Using multi-factor authentication (MFA)  
   c) Storing all passwords in a text document  
   d) Allowing open access to databases  
   **(Answer: b)**
7. **What does encryption do in data security?**  
   a) Deletes unwanted files automatically  
   b) Converts data into unreadable code for protection  
   c) Prevents employees from using the internet  
   d) Speeds up database processing  
   **(Answer: b)**
8. **Why is employee training important for data security?**  
   a) It helps employees identify cyber threats  
   b) It reduces the need for cybersecurity teams  
   c) It guarantees that no cyberattacks will ever happen  
   d) It makes employees responsible for all security issues  
   **(Answer: a)**
9. **What is a key benefit of strong data security?**  
   a) It eliminates the need for IT teams  
   b) It ensures compliance with laws like GDPR and HIPAA  
   c) It allows companies to sell user data freely  
   d) It increases the risk of cyberattacks  
   **(Answer: b)**
10. **Which of the following helps businesses recover from cyberattacks?**  
    a) Disabling security monitoring  
    b) Regular data backups  
    c) Ignoring software updates  
    d) Sharing login credentials freely  
    **(Answer: b)**