

Name _____

Exploring the Security of Cloud Computing

Open-Ended Response Answer Key

1. Individual responsibility in cloud computing security is crucial. Individuals should use strong, unique passwords for their cloud accounts, enable multi-factor authentication when available, and be cautious about sharing sensitive information online. Organizations should educate employees about security best practices and implement strict access controls.
2. Not implementing access controls and strong passwords in cloud computing can lead to unauthorized access to data and resources. Weak access controls can result in data breaches and data loss. For example, the 2019 Capital One data breach occurred due to a misconfigured firewall, highlighting the importance of proper access controls.
3. As a security consultant, I would recommend that the small business implement multi-factor authentication for cloud accounts, regularly update and patch software, conduct employee training on phishing awareness, and regularly audit cloud configurations to identify and mitigate vulnerabilities.
4. Cloud computing security will likely continue to evolve, with advancements in encryption techniques, threat detection, and artificial intelligence. New challenges may arise as cyber threats become more sophisticated, requiring continuous innovation in security measures. The integration of security into the development pipeline (DevSecOps) may also become more prevalent to enhance cloud security.

