**Introduction**

This report will analyse the security posture of ABC Company, a small start-up business providing web development and digital marketing services. The company was founded in 2020 and currently has a staff of five, including the company's founder and CEO. ABC Company is based in the United Kingdom and serves clients around the world.

The main security threats faced by ABC Company are those related to the web development and digital marketing services it provides. These include malicious actors attempting to access the company's client data, malicious code being injected into their websites, and other cyber attacks. Additionally, the company's physical security may be at risk from theft or vandalism.

**ABC Company's Security Roles, Procedures and Management Structures**

ABC Company has established a security policy which outlines the roles, procedures and management structures for the company. The policy is designed to ensure the security of the company's data and systems, and to ensure compliance with applicable regulations.

The company's security roles are divided between the CEO, who is responsible for developing and implementing the security policy, and the IT manager, who is responsible for maintaining the company's IT systems and ensuring their security. The IT manager is also responsible for monitoring the network for security threats and responding to incidents.

The company's security procedures include regular system scans, patching and updating of software, and monitoring of the network for security incidents. The company also has procedures in place for responding to incidents, such as notifying the IT manager, informing clients, and taking corrective action.

The company's security management structure consists of a Security Committee, which is chaired by the CEO and is responsible for overseeing the security policy and procedures. The committee meets regularly to review security issues and provide guidance to the IT manager.

**Network Diagram**

The following network diagram depicts the key locations, departments, and devices within ABC Company. The diagram includes the company's headquarters, where the company's servers and IT systems are located, and the company's remote offices, which are located in different countries around the world.

The company's headquarters is connected to the internet via a router, which provides secure access to the company's servers and systems. The headquarters also has a firewall, which is used to prevent unauthorized access to the network. The remote offices are connected to the internet via a secure VPN, which provides access to the company's servers and systems.

The diagram also includes the company's servers and systems, which are located in the company's headquarters. The servers and systems are protected by a firewall, which is used to prevent unauthorized access. The servers and systems are also monitored by the IT manager, who is responsible for ensuring their security.

The diagram also includes the company's clients, which are located in different countries around the world. The clients are connected to the company's servers and systems through secure VPNs, which provide access to the company's services.

**Risk Analysis Framework**

ABC Company has employed a risk analysis framework to evaluate the company's key security risks. The framework consists of the following steps:

1. Identify security threats: The first step is to identify the security threats that the company faces. This includes identifying potential threats from external sources, such as malicious actors, as well as threats from internal sources, such as poor security practices.

2. Assess risk level: The second step is to assess the level of risk posed by each of the identified threats. This involves evaluating the potential impact of each threat and assigning a risk rating to each threat.

3. Identify mitigation strategies: The third step is to identify mitigation strategies for each of the identified risks. This includes identifying measures that can be taken to reduce the likelihood of the threat occurring, as well as measures to reduce the impact of the threat if it does occur.

4. Implement mitigation strategies: The fourth step is to implement the identified mitigation strategies. This includes implementing technical, human, and physical security measures, as well as any identification and authentication technologies that would be appropriate for the organisation.

5. Monitor and review: The fifth step is to monitor and review the security measures that have been implemented. This includes regularly reviewing the security measures and making changes if necessary.

**Recommendations**

Based on the analysis and findings of the previous sections, the following recommendations are made to improve ABC Company's security posture.

1. Implement a multi-factor authentication system: ABC Company should implement a multi-factor authentication system to protect access to its systems and data. This would involve using a combination of passwords, tokens, biometrics, and other methods to ensure that only authorised users are able to access the company's systems.

2. Implement intrusion detection and prevention systems: ABC Company should also implement intrusion detection and prevention systems to detect and prevent malicious activity on its networks. These systems would monitor the network for suspicious activity and alert the IT manager if any suspicious activity is detected.

3. Implement security policies and procedures: ABC Company should develop and implement security policies and procedures to ensure that its systems and data are protected. These policies and procedures should include procedures for responding to security incidents, as well as procedures for patching and updating software.

4. Educate employees on security issues: ABC Company should ensure that its employees are educated on security issues and made aware of the importance of protecting the company's systems and data. This could be done through security awareness training or by providing employees with resources to help them understand security issues.

5. Implement physical security measures: ABC Company should also implement physical security measures to protect its premises and equipment. This could include using locks and other security devices to prevent unauthorized access, as well as ensuring that the premises are monitored and secure.

**Business Continuity and Disaster Recovery Plan**

ABC Company should develop a business continuity and disaster recovery plan to ensure that its operations can continue in the event of a security incident or disaster. The plan should include procedures for responding to incidents and disasters, as well as procedures for ensuring that data and systems are backed up and can be recovered if necessary. The plan should also include procedures for notifying clients of any incidents or disasters and procedures for restoring operations once the incident or disaster has been resolved.

The plan should also include measures to ensure that the company is able to maintain its operations during an incident or disaster. This could include the use of redundant systems and backup facilities, as well as measures to ensure that the company's operations can continue in the event of a power outage.

**Conclusion**

This report has analysed the security posture of ABC Company and provided recommendations for improving the company's security posture. It has also outlined a business continuity and disaster recovery plan that the company should develop and implement in order to ensure that its operations can continue in the event of a security incident or disaster. The report has highlighted the importance of implementing technical, human, and physical security measures, as well as any identification and authentication technologies that would be appropriate for the organisation to improve their information security.