Introduction:

With the increasing use of technology, businesses have become more reliant on computer systems and networks. However, with this reliance comes an increased risk of cyber-attacks and security breaches. It is important for businesses to understand the potential risks and have measures in place to mitigate against them. This report will provide guidance on the provided network and address some of the major issue of it.

Outdated operating systems and computers:

Using outdated operating systems and computers poses a significant risk to the network. These systems are vulnerable to attacks, which can lead to data loss, legal issues, and financial losses. To mitigate this risk, businesses should update all computers to actively supported and patched operating systems, ensuring they are up-to-date and protected against known vulnerabilities.

In addition to updating operating systems, businesses should implement regular security updates and patches. This approach helps to address any new vulnerabilities and ensures that the system remains secure. By taking these measures, organizations can help ensure that their systems are up-to-date and protected against potential attacks, reducing the risk of data loss, legal issues, and financial losses.

Server located on ground floor:

Network segmentation is crucial to reduce the risk of unauthorized access to sensitive information, malware or virus infection, and difficulty in identifying the source of an attack. Without proper network segmentation, anyone who accesses the network can access all network devices, which can lead to security breaches.

To mitigate this risk, businesses should segment their network to restrict access to certain devices and information. This approach ensures that only authorized personnel have access to sensitive information. Additionally, implementing proper access controls and authentication measures can prevent unauthorized access. Regularly reviewing and monitoring network access logs can also help detect any unauthorized access attempts. By implementing these measures, the business can help ensure the security of their network and protect sensitive information from unauthorized access.

Lack of network segmentation:

Another risk for the business is the lack of network segmentation. If someone can access all network devices on the network, there is a risk of unauthorized access to sensitive information, malware or virus infection, and difficulty in identifying the source of an attack.

To mitigate against this risk, the business should segment the network to restrict access to certain devices and information. This will ensure that only authorized personnel have access to any sensitive information. It is also important to implement proper access controls and authentication measures to prevent unauthorized access. Regularly reviewing and monitoring network access logs will also help identify any unauthorized access attempts.

Weak Authentication:

The use of 15-digit passwords is not strong enough and is simple enough that there is a danger of being brought forced. This could lead to information being leaked by unauthorised individuals.

To mitigate against this risk, the business should implement 2FA (2 factor authentication) being if a password gets compromised it would require the attacker to gain access to the additional factor. On top of this enforcing password complexity and length requirement with rotation polices, will help ensure all people in the company are using strong, hard to guess passwords. Finally, the company should implement monitoring and logging failed passwords to help identify potential unauthorized logon attempts.

Use of Telnet:

Using telnet for remote access to network equipment is not secure and should be replaced with more secure protocols, such as SSH. Failure to do so may result in unauthorized access to network equipment, data theft or loss, and network disruption or downtime.

To enhance security, it is important to implement access control policies that limit access to authorized users. Monitoring and logging remote access sessions can also help identify and prevent security breaches. Regular security audits and vulnerability assessments can further help to identify and mitigate any security risks. In addition to using SSH, these measures can help ensure the security of remote access to network equipment.

Open Source Software:

The use of open-source software can pose security risks due to potential vulnerabilities that may not receive equivalent support as commercial software. The fact that the source code is open for anyone to view may lead to data breaches and legal issues.

To address these concerns, it is crucial to regularly monitor and update open-source software for security vulnerabilities. Along with this, implementing additional security measures such as firewalls and network monitoring can help ensure the system remains secure. For critical systems, using commercial software may be a better option to mitigate potential risks.

Wireless Security:

Although WPA2 is a relatively strong protocol, it is still susceptible to attacks such as password cracking and rogue access point attacks. These attacks can compromise network security, resulting in unauthorized access to the wireless network, theft of confidential data, and disruption of business operations.

To reduce these risks, it is important for businesses to use strong and complex passwords for their wireless network. Additionally, implementing a wireless intrusion detection system can detect rogue access points, while regularly updating firmware and security patches for all wireless access points can help keep the network secure. Enabling additional security measures like MAC address filtering and disabling SSID broadcast will also help further strengthen the security of the wireless network.

Conclusion:

In conclusion, the existing network face a few security risks by implementing the measures outlined in this report, the network can mitigate against these risks and ensure that their systems remain secure. However, the business will need to regularly review the network against new and emerging threats to endure the network’s protection is up to mark.